PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2004-040754

(43)Date of publication of application : 05.02.2004

(51)Int.Cl. H04N 1/387

G06F 17/60

G06T 1/00

G09C 5/00

H04N 5/91

(21)Application number : 2002-362516

(22)Date of filing : 13.12.2002

(71)Applicant : SONY UNITED KINGDOM LTD

(72)Inventor : PELLY JASON CHARLES
TAPSON DANIEL WARREN

(30)Priority

Priority number : 2001 200129840 Priority date : 13.12.2001 Priority country : GB

(54) DATA PROCESSING APPARATUS AND DATA PROCESSING METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To make it difficult for a user who receives the same material to succeed in a collusion attack.

SOLUTION: In a watermark system, an encoded data processing apparatus is provided for creating a watermarked copy of an original material item by introducing one code word in a prescribed set to a copy of an original material item, and the set of code words are generated by shifting a first code word in the manner of circulation. A correlative value of all the code words generated by shifting the first code word is calculated by using a Fourier transformation correlator to remarkably shorten the time required for detecting a code word in the watermarked material

item. The watermark system, is particularly effective for specifying a creation source of a pirate edition copy of a video material produced by photographing watermarked images while using a camcorder in a movie theater, for example.

LEGAL STATUS

[Date of request for examination] 26.10.2005

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

CLAIMS

[Claim(s)]

[Claim 1]

In the coded data processor which generates the copy to which at least one water mark of this original material item was given by introducing one codeword in the group of a predetermined codeword into the copy of an original material item,

The codeword generation machine which generates the codeword which has two or more codeword multipliers,

It has the coding processor which combines the above-mentioned codeword multiplier with the above-mentioned material item,

Two or more codewords in the group of the above-mentioned predetermined codeword are the coded data processors containing the 1st codeword which has two or more 1st codeword multipliers, and other at least one codeword which shifted this 1st codeword cyclically and was generated.

[Claim 2]

The above-mentioned codeword generation machine is a coded data processor according to claim 1 characterized by having the pseudo-random number generation machine which generates the pseudo-random number for deriving the above-mentioned codeword multiplier.

[Claim 3]

The above-mentioned pseudo-random number is a coded data processor according to claim 1 or 2 characterized by being generated by initializing the above-mentioned pseudo-random number generation machine with the seed value which identifies the 1st codeword of the above to a proper.

[Claim 4]

The above-mentioned codeword generation machine is claim 1 characterized by generating the above-mentioned seed value from the sample of the above-mentioned material item thru/or a coded data processor given in 3 any 1 terms.

[Claim 5]

The above-mentioned coding processor is claim 1 characterized by changing the sequence that the above-mentioned codeword multiplier is combined, based on a sequence modification code thru/or a coded data processor given in 4 any 1 terms.

[Claim 6]

The discrete cosine transform processor which changes the above-mentioned material item into a discrete cosine transform field,

The material item of the above-mentioned discrete cosine transform field It is expressed by two or more discrete cosine multipliers. The above-mentioned coding processor By adding one of the above-mentioned codeword multiplier and the corresponding discrete cosine transform multipliers By combining the above-mentioned codeword multiplier and the above-mentioned material item, and carrying out the reverse discrete cosine transform of the image with which the above-mentioned codeword was added by this coding processor and by which the discrete cosine transform was carried out [above-mentioned] A coded data processor [equipped with the reverse discrete cosine transform processor which generates the version to which the water mark of the above-mentioned material item was given] according to claim 6 or 7.

[Claim 7]

Projection equipment equipped with claim 1 which at least one of an audio signal and picture signals is supplied, and introduces a codeword into at least one of this audio signal and picture signals before copy processing thru/or a coded data processor given in 6 any 1 terms.

[Claim 8]

A web server equipped with claim 1 which it is the web server which offers the material item downloaded through the Internet, this material item is supplied before this material item downloads, and introduces a codeword into this material item thru/or a coded data processor given in 6 any 1 terms.

[Claim 9]

The 1st codeword which has two or more predetermined multipliers distributed in pseudo-random, From the group of two or more codewords which consisted of other at least one codeword which shifted cyclically and was generated, this 1st codeword Were generated by combining each codeword multiplier corresponding to each sample of an original material, respectively. In the detection data processor which identifies one or more predetermined codewords which exist in the version to which the water mark of an original material item was given,
The decode processor which reproduces a codeword from the material item to which the above-mentioned water mark was given, and generates a playback codeword,
It has the detection processor which detects at least one codeword from the correlation value exceeding a predetermined threshold of a codeword,
The correlation value of two or more above-mentioned codewords,
The Fourier transform value of the above-mentioned playback codeword is computed,
The Fourier transform value of the 1st codeword of the group of the above-mentioned codeword is computed,
The complex conjugate of either the Fourier transform value of the above-mentioned playback codeword and the Fourier transform value of the codeword by which generation was carried out [above-mentioned] is computed,
The 1st middle product sample is computed by carrying out the multiplication of each Fourier transform sample of the above-mentioned playback codeword, and the Fourier transform sample of the 1st corresponding codeword of the above,
The detection data processor called for by computing the correlation sample to which inverse transformation of the above-mentioned middle product sample is carried out, and each expresses one correlation value in the group of the above-mentioned codeword.
[Claim 10]
The above-mentioned decode processor subtracts the sample to which the version of the material item to which the above-mentioned water mark was given corresponds from the sample of the above-mentioned original material item. The above-mentioned playback codeword is reproduced by subtracting the sample to which the version to which the above-mentioned water mark was given corresponds from the sample of the above-mentioned original material item. The detection data processor according to claim 9 characterized by generating total of a correlation value about each of two or more above-mentioned codewords by investigating correlation with the above-mentioned playback codeword and this each codeword.
[Claim 11]
A detection data processor [equipped with the registration processor which relates the sample of the version to which the water mark of the above-mentioned original material item was given with the sample to which the original material item with which the above-mentioned codeword multiplier which carries out correspondence

was combined corresponds] according to claim 9 or 10.
[Claim 12]
The above-mentioned correlation processor is claim 9 characterized by having the codeword generation machine which generates the above-mentioned seed value from the material item to which the above-mentioned water mark was given thru/or a detection data processor given in 11 any 1 terms.
[Claim 13]
It is introduced into a material item in a discrete cosine transform field, and the above-mentioned codeword is the detection data processor concerned,
When it has the discrete cosine transform processor which changes into a discrete cosine transform field the version to which the above-mentioned water mark was given, and an original material item and the above-mentioned playback processor subtracts the discrete cosine transform multiplier to which the version to which the above-mentioned water mark was given corresponds from the discrete cosine transform multiplier of the above-mentioned original material item, they are claim 9 characterized by generating the above-mentioned playback codeword thru/or a detection data processor given in 12 any 1 terms.
[Claim 14]
In the addressee specification system which specifies the addressee of a material item,
Claim 1 which generates the material item to which the water mark was given by introducing into a material item the codeword generated from the seed value which specifies the above-mentioned addressee as a proper thru/or a coded data processor given in 6 any 1 terms,
An addressee specification system equipped with claim 9 which detects the addressee of this material item by predetermined incorrect detection probability by detecting the existence of the codeword in the above-mentioned material item thru/or a detection data processor given in 13 any 1 terms.
[Claim 15]
In the coding approach which generates the copy to which at least one water mark of this original material item was given by introducing one codeword in the group of a predetermined codeword into the copy of an original material item,
The step which generates the codeword which has two or more codeword multipliers,
It has the step which combines the above-mentioned codeword multiplier with the above-mentioned material item,
The step which generates the above-mentioned codeword,
The step which generates the 1st codeword which has two or more 1st codeword multipliers,
The coding approach of having the step which shifts this 1st codeword cyclically and generates other at least one codeword.
[Claim 16]
In the discernment approach of identifying the group of one or more predetermined

codewords which exist in the version to which the water mark of an original material item was given generated by combining each codeword multiplier corresponding to each sample of the copy of an original material, respectively,
The step which reproduces a codeword from the material item to which the above-mentioned water mark was given, and generates a playback codeword,
It has the step which detects at least one codeword from the correlation value exceeding a predetermined threshold of a codeword,
The correlation value of two or more above-mentioned codewords,
The Fourier transform value of the above-mentioned playback codeword is computed,
The Fourier transform value of the 1st codeword of the group of the above-mentioned codeword is computed,
The complex conjugate of either the Fourier transform value of the above-mentioned playback codeword and the Fourier transform value of the codeword by which generation was carried out [above-mentioned] is computed,
The 1st middle product sample is computed by carrying out the multiplication of each Fourier transform sample of the above-mentioned playback codeword, and the Fourier transform sample of the 1st corresponding codeword of the above,
The discernment approach searched for by computing the correlation sample to which inverse transformation of the above-mentioned middle product sample is carried out, and each expresses one correlation value in the group of the above-mentioned codeword.
[Claim 17]
The data signal showing the material item to which the codeword was added by claim 1 thru/or the coded data processor given in 6 any 1 terms.
[Claim 18]
Data medium with which the data signal according to claim 17 was recorded.
[Claim 19]
The computer program which offers the instruction which can be executed by computer which it is loaded [computer] to a data processor and operates this data processor as claim 1 thru/or a coded data processor given in 6 any 1 terms or claim 9 thru/or a detection data processor given in 13 any 1 terms.
[Claim 20]
The computer program which offers the instruction which can be executed by computer which it is loaded [computer] to a data processor and makes this data processor perform an approach according to claim 15 or 16.
[Claim 21]
The computer program product equipped with the medium which can be read by computer by which the information signal showing a computer program according to claim 19 or 20 is recorded.
[Claim 22]
The receiving set which combines with this input signal at least one codeword which

multiplier with a material item. Two or more codewords in the group of a predetermined codeword contain the 1st codeword which has two or more 1st codeword multipliers, and other at least one codeword which shifted this 1st codeword cyclically and was generated.

[0010]

This invention aims at offering the realistic water mark system using the codeword which has a multiplier which is indicated by U.S. Pat. No. 5664018, and which was distributed at random. In order to realize an effective system actually, the larger possible one of the number of codewords discriminable to a proper is good. a distribution to consumer appliances, such as video equipment, the projector for movie theaters, etc. sake -- millions -- it is necessary to prepare the group of tens of millions of codewords preferably Here, the processing which the group of the codeword which consists of 10 million codewords is generated [processing], and makes each generated codeword and a playback codeword correlate serves as a big processing burden. even if it uses a high performance computer -- **** with such unreal correlation processing -- even if few, time amount long like a user senses as inconvenience is required. By the example of this invention, correlation over the codeword of a lot can be calculated efficiently. By this example, among the groups of a codeword, some [at least] codewords generate the 1st codeword, and are generated by computing other codewords by shifting this 1st codeword cyclically. Thereby, the correlation value of all the codewords in a group is computable using Fourier transform correlator. Fourier transform correlator computes the correlation value of a lot by one processing, and mitigates an operation task substantially so that it may mention later.

[0011]

Moreover, the detection data processor concerning this invention reproduces a codeword from the material item to which the water mark was given, and is equipped with the decode processor which generates a playback codeword, and the detection processor which detects at least one codeword. A codeword is detected based on the correlation value computed by making it correlate with each of two or more codewords which had the restored codeword generated. That is, a corresponding codeword is detected when a correlation value exceeds a predetermined threshold. This correlation value computes the Fourier transform value of a playback codeword, and computes the Fourier transform value of the 1st codeword of the group of a codeword. The complex conjugate of either the Fourier transform value of a playback codeword and the Fourier transform value of the generated codeword is computed. The 1st middle product sample is computed by carrying out the multiplication of each Fourier transform sample of a playback codeword, and the Fourier transform sample of the 1st corresponding codeword. Inverse transformation of the middle product sample is carried out, and it asks by computing the correlation sample to which each expresses one correlation value in the group of a codeword.

[0012]

In a suitable example, a coding processor changes the sequence that the above-mentioned codeword multiplier is combined, based on a sequence modification code. Corresponding to this, a detection data processor computes a correlation value by returning the sequence of the generated codeword multiplier or a playback codeword multiplier in a suitable example. Although the probability for a KORUJON attack to be successful by shifting the 1st codeword cyclically becomes high, this probability can be reduced by changing the sequence of a codeword multiplier.

[0013]

The further side face and the further description of this invention are defined in the attached claim.

[0014]

[Embodiment of the Invention]

A general view of a water mark system

Hereafter, the gestalt of operation of this invention is related to protection of a video image, and it explains. The number of copies is determined by the number of the users who should distribute a video image. The discernment codeword (identification code word) for identifying the copy assigned to one of these users is added to each copy.

[0015]

A video image is one example of the material protected by embedding a digital codeword. The material protected by embedding a codeword may be a material including a software program, a digital document, music, an audio signal, and what other kinds of information other than a video image.

[0016]

Drawing 1 is the block diagram showing the concrete configuration of the coded-image processor (encoding image processing apparatus) which introduces a discernment codeword into the copy of an original image. The original image I is supplied from the source and saved at a frame memory 1. This original image is copied as two or more copies to which the water mark was given (reproduce), and the discernment codeword of a proper is given to each copy. An original image is supplied to the DCT processor 2, and the DCT processor 2 divides an original image into the pixel block of 8x8, and performs DCT processing to each pixel block of 8x8. Thereby, the DCT processor 2 generates the DCT resolution picture V.

[0017]

In the following explanation, the vocabulary a "sample" shall point out the discrete sample which constitutes an image (or you may be the material of other classes in fact.). A sample may be a brightness sample of the image which can be copied also from a pixel. Therefore, vocabulary called a sample and vocabulary called a pixel may be exchangeable depending on a situation.

[0018]

The DCT image V is supplied to the coding processor (henceforth an encoder) 4. The discernment codeword is also supplied to the coding processor 4 from the

discernment codeword generation machine 8.
[0019]
Two or more seed values (seed) are supplied to the discernment codeword generation machine 8. Each seed value is used in order to generate one of the discernment codewords which correspond, respectively. Each generated discernment codeword is embedded to the copy of an original image, and the image to which the water mark was given by this is generated. The discernment codeword generation machine 8 is equipped with a pseudo-random number generation machine. A pseudo-random number generation machine generates the codeword multiplier for forming a specific discernment codeword. In a desirable example, a codeword multiplier is generated based on normal distribution. In addition, it may replace with this and a codeword multiplier may be beforehand defined based on the seed value used since a pseudo-random number generation machine is initialized. Therefore, a corresponding seed value exists in each discernment codeword, and each seed value is memorized by memory 12. That is, in order to generate the discernment codeword Xi, the seed value seedi is read from memory 12, and the pseudo-random number generation machine in the discernment codeword generation machine 8 is initialized using this seed value seedi.
[0020]
The DCT version of an original image is expressed in the following explanation as V. It is here,
V={vi}= {v1, v2, v3, v4, ..., vN}
It comes out, and it is and vi is the DCT multiplier of an image. In other examples, vi is the sampled value of an image and may express the sampled value of the image in the sampled value of an image in a space field, or other fields.
[0021]
Each discernment codeword Xi consists of codeword multipliers of n pieces as follows.
Xi={xij}= {xi1, xi2, xi3, xi4, ..., xin}
Several n of a codeword multiplier corresponds to the measurement size of the original image V. In addition, the number of multipliers may differ and this number may be determined according to specific application.
[0022]
And the vector of the codeword multiplier which constitutes the i-th discernment codeword Xi is supplied to an encoder 4 through a channel 14. An encoder 4 generates the image Wi to which the water mark was given by adding the discernment codeword Xi to Image V. In fact, as shown in the following formulas, the image Wi to which the water mark was given is generated by applying each codeword multiplier to each multiplier of an image.
Wi=V+Xi
Wi=v1+xi1, v2+xi2, v3+xi3, v4+xi4, ..., vn+xin
As shown in drawing 1 , the image Wi to which the water mark was given is

outputted by it from this image processing system, after reverse DCT conversion is carried out by the reverse DCT processor 18 which carries out reverse DCT conversion of the image generated by the encoder 4.

[0023]

Therefore, as shown in drawing 1 , from an encoder 4, the group of the image to which the water mark was given is outputted. If data word is made into a maximum of 20 bits, one of the 10 million discernment codewords can be chosen, and the version Wi to which 10 million water marks were given can be generated to an original image.

[0024]

Although the copy Wi to which the water mark of Image I was given is discriminable according to an individual with this discernment codeword, in other examples, data can be sent within an image by above-mentioned 20 bits. Therefore, 20 bits of payloads of 20 bits for sending data within Image V used in order to choose a discernment codeword so that it may explain below are offered.

[0025]

The coded-image processor which is shown in drawing 1 and which generates the image to which the water mark was given is built into various products in various different scenarios with which this invention is applied. For example, a coded-image processor can be connected to a website or a web server, and the image to which the water mark was given can be downloaded. Before downloading the copy of an image, the codeword of a proper is introduced into the image to download and the codeword of this proper can detect the addressee of the downloaded image behind.

[0026]

In other examples of application, a coded-image processor is incorporated as some digital projectors (digital cinema projector), and in a movie theater, in case a discernment codeword projects a movie, it is added to an image. By this discernment codeword, the projector and movie theater which the movie projected can be pinpointed. Therefore, the projector and movie theater where the pirate edition copy was created can be pinpointed by the discernment codeword contained in the pirate edition copy which photoed the image projected from the projector and was obtained. On the other hand, the image to which the water mark was given may be copied as a photograph or printed matter, and may create and distribute the copy of the copied photograph or printed matter. In drawing 1 , the distribution place of the image to which the water mark generated by the coded-image processor was given is shown by the distribution 19 expressed by the cloud-shaped frame.

[0027]

Detection processor

Drawing 2 is the block diagram showing the configuration of the detection image processing system (detecting image processing apparatus) which detects one or more codewords currently embedded in the OFENDINGU image (offending markedimage) to which the water mark was given. Speaking comprehensively, the

detection image processing system shown in drawing 2 having the function to identify one or more codewords which exist in OFENDINGU of an image, i.e., a copy.
[0028]
OFENDINGU version W' of the image to which the water mark was given is supplied from the source of data, and is saved at a frame memory 20. Since the detection processing in this detection image processing system needs the original version of an image, the original version of an image is saved at the frame memory 24. The original version of OFENDINGU version W' of the image to which the water mark was given, and an image is supplied to the registration processor (registration processor) 30 through the connection channels 26 and 28 according to individual, respectively.
[0029]
As mentioned above, OFENDINGU version W' of an image may have been generated by photoing or copying some images Wi to which the water mark was given. Then, in order to raise the detection ratio of a discernment codeword, the registration processor 30 arranges substantially the original version of the OFENDINGU image saved at frame memories 20 and 24, respectively, and an image (align). This purpose is investigating correspondence relation with the sample of the corresponding image Wi with which Sample I and the water mark of an original image are attached, and the codeword multiplier's is added.
[0030]
This registration processing is explained using drawing 3 . Drawing 3 compares OFENDINGU version W' of the original image I and the image to which the water mark was given, and is shown. As shown in drawing 3 , OFENDINGU version W' of the image to which the water mark was given has offset to the original image, and this offset may originate in the relative visual field of a camera that the OFENDINGU version of the image to which the water mark was given was generated.
[0031]
In order to reproduce the expression of a codeword multiplier, it is necessary to subtract the right sample of an original image from OFENDINGU version W' of the image to which the water mark was given. Two images are arranged for this processing. As shown in drawing 3 , registered image W″ has the boundary region (peripheral area) PA which contains in an original image the part not existing.
[0032]
By other examples, when an OFENDINGU version downloads, for example from the Internet, correspondence relation with the version I of an original image may already be in **, and, in such a case, it is not necessary to use the registration processor 30 with OFENDINGU image W'. Then, this detection image processing system is equipped with the alternative-channel 32 for supplying directly the image to which the water mark was given to the playback processor 40.
[0033]
Registered image W″ is supplied to the playback processor 40. The copy of the original image I is also supplied to the playback processor 40 through the 2nd

channel 44. Image W″ and the original image I which were registered are changed into a DCT field by the DCT processor 46. Next, as shown in the following formulas, presumed codeword X' is computed by subtracting sample V' of the DCT field of the image to which the water mark was given from the sample V of the DCT field of an original image.

X'=V'-V

= v'1-v1, v'2-v2, v'3-v3, v'4-v4, ..., v'n-vn

= x'1, x'2, x'3, x'4, ..., x'n

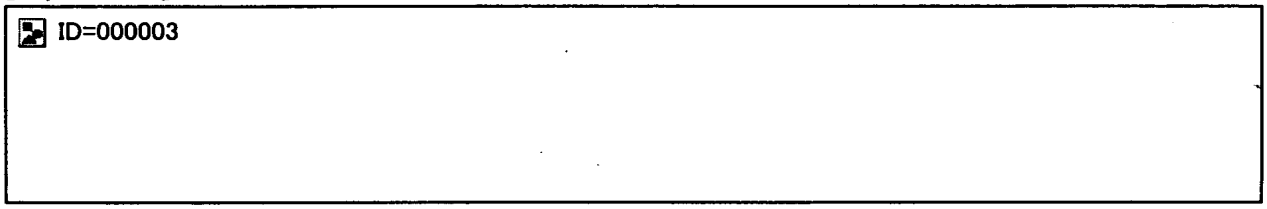
Therefore, the playback processor 40 outputs the estimate of the multiplier of the codeword which should be identified through the connection channel 50. Reproduced codeword X' is supplied to the 1st input terminal of correlator 52. The codeword Xi generated with the codeword generation vessel 54 is supplied to the 2nd input terminal of correlator 52. The codeword generation machine 54 generates the group of all possible codewords using the predetermined seed value which identifies to a proper the codeword read from memory 58 like the above-mentioned discernment codeword generation machine 8.

[0034]

Correlator 52 generates the similar value sim of n pieces (i). In one example, the similar value sim (i) is computed by searching for the correlation based on the following formulas.

[0035]

[Equation 1]



[0036]

Each of the similar value sim of n pieces (i) is supplied to a detector 60. and a detector 60 analyzes the similar value sim of n possible codewords (i) which is alike, respectively and receives. The relation between the example of the similar value sim (i) generated by correlator 52 and the threshold TH of each possible codeword is shown in drawing 4 . As shown in drawing 4 , two codewords 2001 and 12345 are over the threshold TH. For this reason, a detector 60 judges with the OFENDINGU image having been created from the version of the image to which the water mark corresponding to a codeword 2001 and a codeword 12345 was given. Therefore, in this example, the height of the threshold TH which guarantees incorrect detection probability can be set up based on the incorrect detection probability (false positive probability) determined with the magnitude of the population which is 10 million, and

water mark reinforcement (watermarking strength). By the example shown in drawing 4 , when the similar value generated by correlator 52 is over the threshold, it has this incorrect detection probability, the addressee of the image to which this water mark was given performs a malfeasance, and it is judged that it participated in creation of the OFENDINGU version Wi of the image to which the water mark was given.

[0037]

Hereafter, the water mark system feature and advantage which are shown in drawing 1 and drawing 2 are explained.

[0038]

Registration

The processing which arranges the OFENDINGU version of the image to which the water mark was given, and the copy of an original image includes the processing which investigates correlation with the sample of an original image, and the sample of the image to which the water mark was given. This correlation processing is performed by shifting each sample of an image by different shift amount. This processing is explained using drawing 5 . Drawing 5 A shows the discrete sample of an original image, and drawing 5 B shows the discrete sample of OFENDINGU image W' to which the water mark was given. As shown in drawing 5 A and drawing 5 B, the time difference between each sample is dt which becomes settled with a sampling rate. The group of each sample of these images is shifted and the result of having made the discrete sample correlating is shown in drawing 5 C.

[0039]

As shown in drawing 5 C, the correlation peak is the highest between the 6th sample and the 7th sample. Then, to an original image, only this amount is shifted and the OFENDINGU image to which the water mark was given is registered.

[0040]

Fourier decode

The water mark system mentioned above with reference to drawing 1 and drawing 2 can create the version to which 10 million water marks were given to the original image. This is realized by using the water mark value of 20 bits. Here, in order to detect existence of the codeword in the OFENDINGU image to which the water mark was given among two or more codewords as mentioned above, it is necessary to investigate correlation with the codeword reproduced from the image, and each 10 million possible codeword. Such an operation task serves as a big processing burden.

[0041]

The correlator based on this invention shortens time amount required in order to detect the codeword in the OFENDINGU image to which the burden of this data processing was mitigated, therefore the water mark was given. This correlator based on this invention is shown in drawing 6 . The correlator shown in drawing 6 offers effective technique on the alternative target to calculation of total of the correlation

value mentioned above. That is, by this example, total of a correlation value is computed based on the following formulas.

$F-1[F(X')F(x(1))*]$

Here, F (A) expresses the Fourier transform of A and F-1 (A) expresses the inverse Fourier transform of A.

[0042]

The correlator 52 shown in drawing 6 is equipped with the 1st Fourier transform processor 100 and the 2nd Fourier transform processor 102. The 1st and 2nd Fourier transform processors 100 and 102 may be realized using a fast-Fourier-transform algorithm. The 2nd Fourier transform processor 102 also computes the complex conjugate X1 of the Fourier transform value of the generated codeword. The complex conjugate X1 of Fourier transform value X' of a playback codeword and the Fourier transform of the generated codeword is supplied to the 1st and 2nd input terminals of a multiplier 110, respectively. A multiplier 110 carries out the multiplication of each sample from the Fourier transform processors 100 and 102, and supplies this result to the inverse Fourier transform processor 112. From this correlator 52, the inverse Fourier transform value of the signal sample by which multiplication was carried out is outputted.

[0043]

Thus, in the correlator 52 shown in drawing 6 , time amount required in order to compute correlation with n codewords Xi and playback codeword X' which were generated is shortened. This is because fast-Fourier-transform integrated circuits, such as an application-specific integrated circuit (application specific integrated circuit:ASIC) marketed, for example, can constitute the Fourier transform processors 100, 102, and 112. Furthermore, the inverse Fourier transform value outputted from correlator 52 offers the similar value sim of n pieces corresponding to total of the correlation value of n pieces (i). Here, in order to use the property of the correlator 52 shown in drawing 6 , the codeword is generated by shifting one generated codeword X (1) cyclically using the specific seed value supplied to a random-number generation machine. Hereafter, generation of this codeword is explained. The 1st codeword X (1) is expressed as values x1-xn corresponding to the numeric value generated in pseudo-random with the codeword generation vessel 8 so that it may mention later. On the other hand, the 2nd codeword X (2) is generated by performing the cyclic shift to the 1st codeword X (1). Furthermore, as shown below, other codewords are generated by shifting the 1st codeword X (1) cyclically until the n-th codeword is shifted to the location of n-1.

$X(1)=(x1,x2,x3,x4...,xn-1,xn)$

$X(2)=(x2,x3,x4...,xn-1,xn,x1)$

$X(3)=(x3,x4...,xn-1,xn,x1,x2)$

...

$X(n)=(xn,x1,x2,x3,x4...,xn-2,xn-1)$

The correlator 52 which performs the Fourier transform can compute all the similar

values about all n codewords by one processing by constituting a part or all of a group of a codeword that is generated by the coded-image processor using the group of this codeword. Therefore, the total sim of the similar value of n pieces (i) is generated as mentioned above by the shift to which it corresponds from 1 to an original codeword to n, and as shown in drawing 4 , the total sim of a big similar value (i) is generated about at least one codeword. Thus, correlator 52 can receive only one generated codeword corresponding to the 1st codeword X (1), and as shown in drawing 4 , it can compute the similar value about the group of n codewords.

[0044]

If the sample contained in a codeword like [it is ****** and] from the above explanation is N individual, a possible circular shift is only N individual. Therefore, if the population p of a required codeword is larger than N, the water mark used as two or more foundations is needed. The water mark used as each foundation is shifted cyclically, and the peculiar codeword of N individual is generated.

[0045]

When the image to which the water mark was given constitutes one of two or more of the images, such as for example, a video sequence, the same codeword can be given to each image. Therefore, if the codeword under one judgment (suspected code word) is specified using the Fourier transform correlator shown in drawing 6 , even if it uses the total sim of a perfect correlation value (i) as mentioned above, the correlation value which follows is computable. What is necessary is here, to perform correlation processing only to the codeword specified by the Fourier transform correlator shown in drawing 6 , since the codeword under judgment is already specified.

[0046]

Moreover, the complex conjugate of the Fourier transform value of a playback codeword may be computed instead of computing the complex conjugate of the Fourier transform value of the 1st generated codeword X1. This processing is expressed as the 2nd modification of processing by the Fourier transform correlator shown below.

$F-1[F(X')*F(x(1))]$

Thus, either the complex conjugate of the Fourier transform value of a playback codeword and the Fourier transform value of the generated codeword are computed by either of the Fourier transform processors 100 and 102.

[0047]

Secret sequence modification of a codeword

There is a problem that the security of a water mark falls, by the technique of making shift the 1st codeword X1 cyclically, and generating a codeword. This is because two images to which the water mark was given are compared in a KORUJON attack. When the codeword which are two versions of the same codeword which was made to shift the same codeword cyclically and generated it is

added to each image, those who try a KORUJON attack specify the difference between 2 materials to which the water mark was given, therefore it becomes easy to specify a codeword. If those who try a KORUJON attack can specify a codeword, this person can remove a water mark, or can alter a water mark, and can pretend to be the others.

[0048]

In order to prevent such a KORUJON attack, by this example, the sequence of each codeword multiplier of each codeword shifted cyclically is changed at random based on the secret sequence modification code (secret permutation code) pi. A sequence change of a codeword multiplier is made secret to the addressee of the image to which the water mark was given. It becomes difficult for those who try a KORUJON attack to specify by this correlation between two images to which the water mark was given, and possibility that a KORUJON attack will be successful falls.

[0049]

In a detection data processor, the secret sequence exchange code pi is known. In a detection data processor, correlation processing is performed, after performing reverse-order exchange pi- to the codeword multiplier or playback codeword multiplier which the codeword generation machine or the restoration processor 40 generated. The actuation of a detection data processor shown in the coding data processor and drawing 2 which are shown in drawing 1 is shown in drawing 7 and drawing 8 , respectively.

[0050]

Codeword generation

By generating the seed value of the random number used in order to generate a codeword from a source image sample, the engine performance of the example of this invention shown in drawing 1 and drawing 2 can be raised further. This processing analyzes the DCT multiplier of the image which should attach a water mark, and is realized by generating the seed value used from these DCT multipliers in order to generate a codeword. The "secure hash algorithm 1 (secure hashing algorithm 1:sha-1)" of the common knowledge for for example, this contractor can be used for this processing. This algorithm is specified to ANSI Standaards (ANSI x 9.30-2). This algorithm is indicated by A Jay Menezes (A. J.Menezes) work "an application cryptography handbook (Handbook of applied cryptography)." Thereby, a coded-image processor and a detection image processing system can generate and judge the seed value of a random number from a DCT multiplier.

[0051]

Other examples of application

In addition to the projector and web server which were mentioned above, the coded data processor of a water mark system is applicable to other applications. For example, this invention can receive a signal from a communication device, and can apply it also to the receiver/decoder which gives a water mark to information by introducing a codeword into this received signal. For example, a set top box receives

television and a video signal from the "head end" device or multicast device of broadcast. In such an example of application, a coded data processor constitutes a part of set top box, and in case it receives and decodes a signal, it introduces a water mark codeword into a video signal. Setting in one example, this water mark codeword specifies the set top box which received and decoded the video signal as a proper.

[0052]

Furthermore, this invention is applicable also to the digital cinema receiver which receives digital cinema data (digital cinema film) from a satellite. This digital cinema receiver receives the signal showing a digital cinema, decodes this signal, and reproduces a digital cinema. This receiver is equipped with the coded data processor which introduces a water mark codeword into the decoded movie signal. A water mark codeword specifies the digital cinema receiver which received for example, digital cinema data as a proper.

[0053]

Furthermore, this invention is applicable to a digital camera or a camcorder equipped with memory and a memory controller etc. In this example of application, the coded data processor concerning this invention introduces the water mark codeword memorized by memory into the video signal photoed with the digital camera etc. In this example of application, the codeword is beforehand memorized by memory, therefore the coded data processor is not equipped with the codeword generation machine. The codeword memorized by memory is embedded under control of a memory controller at a video signal, and, thereby, specifies a video signal as a false proper target (quasi-uniquely) peculiar.

[0054]

In the further example, the coded data processor based on this invention embeds a series of water mark codewords according to an individual at each of the frame of the digital image from which the plurality which constitutes a continuous image or a continuous animation differs. These codewords may have relevance mutually and can identify now the image corresponding to each frame according to an individual by these codewords.

[0055]

The further various side faces and descriptions of this invention are defined in the attached claim. The gestalt of operation mentioned above can be changed variously, without deviating from this claim.

[Brief Description of the Drawings]

[Drawing 1] It is the block diagram showing the configuration of a coded-image processor.

[Drawing 2] It is the block diagram showing the configuration of a detection image processing system.

[Drawing 3] Drawing 3 A shows an original image, drawing 3 B shows the image to which the water mark was given, and drawing 3 C is drawing showing the registered

image.
[Drawing 4] It is the graphical representation showing the example of the correlation result about each codeword of the group of the codeword of N individual.
[Drawing 5] Drawing 5 A is a graphical representation corresponding to the sample of the original image I, drawing 5 B is a graphical representation corresponding to image W' to which the water mark was given, and drawing 5 C is the graphical representation showing the correlation result for every discrete sample shift of an original image and the image to which the water mark was given.
[Drawing 6] It is the block diagram showing the configuration of the correlator which is a part of detection data processor shown in drawing 2 .
[Drawing 7] It is the flow chart which shows the procedure which creates the image to which the water mark was given by the coded-image data processor.
[Drawing 8] It is the flow chart which shows the processing which specifies a water mark from the image to which the water mark which received was given by the detection data processor shown in drawing 2 .

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1] It is the block diagram showing the configuration of a coded-image processor.
[Drawing 2] It is the block diagram showing the configuration of a detection image processing system.
[Drawing 3] Drawing 3 A shows an original image, drawing 3 B shows the image to which the water mark was given, and drawing 3 C is drawing showing the registered image.
[Drawing 4] It is the graphical representation showing the example of the correlation result about each codeword of the group of the codeword of N individual.
[Drawing 5] Drawing 5 A is a graphical representation corresponding to the sample of the original image I, drawing 5 B is a graphical representation corresponding to image W' to which the water mark was given, and drawing 5 C is the graphical representation showing the correlation result for every discrete sample shift of an original image and the image to which the water mark was given.
[Drawing 6] It is the block diagram showing the configuration of the correlator which is a part of detection data processor shown in drawing 2 .
[Drawing 7] It is the flow chart which shows the procedure which creates the image to which the water mark was given by the coded-image data processor.
[Drawing 8] It is the flow chart which shows the processing which specifies a water

mark from the image to which the water mark which received was given by the detection data processor shown in drawing 2 .

(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2004-40754
(P2004-40754A)
(43)公開日　平成16年2月5日(2004.2.5)

(51)Int.Cl.[7]		F I			テーマコード（参考）
H04N	1/387	H04N	1/387		5B057
G06F	17/60	G06F	17/60	302E	5C053
G06T	1/00	G06F	17/60	512	5C076
G09C	5/00	G06T	1/00	500B	5J104
H04N	5/91	G09C	5/00		

審査請求 未請求　請求項の数 24　OL　外国語出願　（全 42 頁）　最終頁に続く

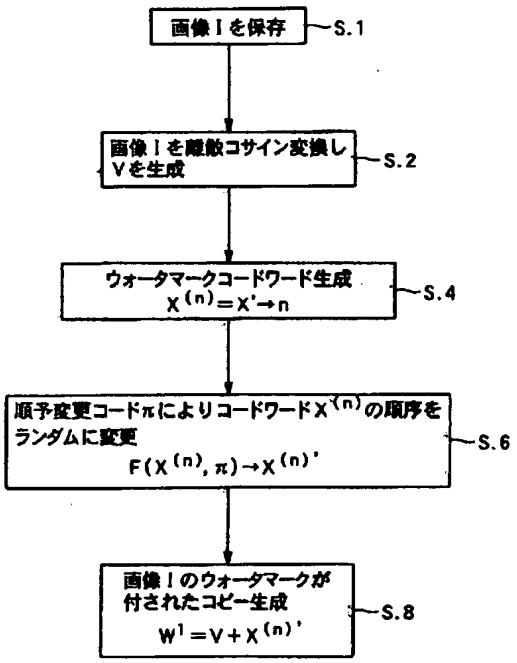
(21)出願番号　特願2002-362516(P2002-362516)
(22)出願日　平成14年12月13日(2002.12.13)
(31)優先権主張番号　0129840.5
(32)優先日　平成13年12月13日(2001.12.13)
(33)優先権主張国　イギリス(GB)

(71)出願人　593081408
ソニー・ユナイテッド・キングダム・リミテッド
Sony United Kingdom Limited
イギリス国　サリー，ウェーブリッジ，ブルックランズ，ザ　ハイツ（番地なし）
(74)代理人　100067736
弁理士　小池　晃
(74)代理人　100086335
弁理士　田村　榮一
(74)代理人　100096677
弁理士　伊賀　誠司

最終頁に続く

(54)【発明の名称】データ処理装置及びデータ処理方法

(57)【要約】　（修正有）
【課題】同じマテリアルを受け取ったユーザーコルージョンアタックに成功することが困難になるようにする。
【解決手段】ウォータマークシステム、オリジナルマテリアルアイテムのコピーに所定の組のうちの１つのコードワードを導入し、オリジナルマテリアルアイテムのウォータマークが付されたコピーを生成する符号化データ処理装置を備え、コードワードの組は、第１のコードワードを循環的にシフトさせて生成される。フーリエ変換相関器を用いて、第１のコードワードをシフトすることにより生成された全てのコードワードの相関値を算出し、ウォータマークが付されたマテリアルアイテム内のコードワードを検出するために要する時間を大幅に短縮する。このウォータマークシステムは、例えば映画館においてカムコーダを用いてウォータマークが付された画像を撮影することにより作成された映像マテリアルの海賊版コピーの作成元を特定する場合等に特に有効である。
【選択図】　図７



【特許請求の範囲】
【請求項１】
オリジナルマテリアルアイテムのコピーに所定のコードワードの組のうちの１つのコードワードを導入することにより、該オリジナルマテリアルアイテムの少なくとも１つのウォータマークが付されたコピーを生成する符号化データ処理装置において、
複数のコードワード係数を有するコードワードを生成するコードワード生成器と、
上記コードワード係数を上記マテリアルアイテムに結合する符号化プロセッサとを備え、
上記所定のコードワードの組内の複数のコードワードは、第１の複数のコードワード係数を有する第１のコードワードと、該第１のコードワードを循環的にシフトして生成された少なくとも１つの他のコードワードとを含む符号化データ処理装置。
【請求項２】
上記コードワード生成器は、上記コードワード係数を導出するための疑似乱数を生成する疑似乱数生成器を備えることを特徴とする請求項１記載の符号化データ処理装置。
【請求項３】
上記疑似乱数は、上記第１のコードワードを固有に識別するシード値により上記疑似乱数生成器を初期化することにより生成されることを特徴とする請求項１又は２記載の符号化データ処理装置。
【請求項４】
上記コードワード生成器は、上記マテリアルアイテムのサンプルから上記シード値を生成することを特徴とする請求項１乃至３いずれか１項記載の符号化データ処理装置。
【請求項５】
上記符号化プロセッサは、順序変更コードに基づいて、上記コードワード係数が結合される順序を変更することを特徴とする請求項１乃至４いずれか１項記載の符号化データ処理装置。
【請求項６】
上記マテリアルアイテムを離散コサイン変換領域に変換する離散コサイン変換プロセッサと、
上記離散コサイン変換領域のマテリアルアイテムは、複数の離散コサイン係数によって表現され、上記符号化プロセッサは、上記コードワード係数と対応する離散コサイン変換係数の１つとを加算することにより、上記コードワード係数と上記マテリアルアイテムとを結合し、該符号化プロセッサによって上記コードワードが加算された上記離散コサイン変換された画像を逆離散コサイン変換することにより、上記マテリアルアイテムのウォータマークが付されたバージョンを生成する逆離散コサイン変換プロセッサとを備える請求項６又は７記載の符号化データ処理装置。
【請求項７】
オーディオ信号及び画像信号のうちの少なくとも１つが供給され、複写処理の前に該オーディオ信号及び画像信号のうちの少なくとも１つにコードワードを導入する請求項１乃至６いずれか１項記載の符号化データ処理装置を備える映写装置。
【請求項８】
インターネットを介してダウンロードされるマテリアルアイテムを提供するウェブサーバであって、該マテリアルアイテムがダウンロードされる前に該マテリアルアイテムが供給され、該マテリアルアイテムにコードワードを導入する請求項１乃至６いずれか１項記載の符号化データ処理装置を備えるウェブサーバ。
【請求項９】
疑似ランダム的に分布した複数の所定係数を有する第１のコードワードと、該第１のコードワードを循環的にシフトして生成された少なくとも１つの他のコードワードとから構成された複数コードワードの組から、オリジナルマテリアルの各サンプルに、それぞれ対応する各コードワード係数を結合することにより生成された、オリジナルマテリアルアイテムのウォータマークが付されたバージョン内に存在する１つ以上の所定のコードワードを識別する検出データ処理装置において、

上記ウォータマークが付されたマテリアルアイテムからコードワードを再生し、再生コードワードを生成する復号プロセッサと、
所定の閾値を超えるコードワードの相関値から少なくとも１つのコードワードを検出する検出プロセッサとを備え、
上記複数のコードワードの相関値は、
上記再生コードワードのフーリエ変換値を算出し、
上記コードワードの組の第１のコードワードのフーリエ変換値を算出し、
上記再生コードワードのフーリエ変換値及び上記生成されたコードワードのフーリエ変換値のいずれか一方の複素共役を算出し、
上記再生コードワードの各フーリエ変換サンプルと対応する上記第１のコードワードのフーリエ変換サンプルとを乗算して第１の中間積サンプルを算出し、
上記中間積サンプルを逆変換し、それぞれが上記コードワードの組のうちの１つの相関値を表す相関サンプルを算出することにより求められる検出データ処理装置。
【請求項１０】
上記復号プロセッサは、上記オリジナルマテリアルアイテムのサンプルから上記ウォータマークが付されたマテリアルアイテムのバージョンの対応するサンプルを減算し、上記オリジナルマテリアルアイテムのサンプルから上記ウォータマークが付されたバージョンの対応するサンプルを減算することにより上記再生コードワードを再生し、上記複数のコードワードのそれぞれについて、上記再生コードワードと該各コードワードとの相関を調べることにより相関値の総和を生成することを特徴とする請求項９記載の検出データ処理装置。
【請求項１１】
上記オリジナルマテリアルアイテムのウォータマークが付されたバージョンのサンプルを、上記対応するコードワード係数が結合されたオリジナルマテリアルアイテムの対応するサンプルに関連付ける登録プロセッサを備える請求項９又は１０記載の検出データ処理装置。
【請求項１２】
上記相関プロセッサは、上記ウォータマークが付されたマテリアルアイテムから上記シード値を生成するコードワード生成器を備えることを特徴とする請求項９乃至１１いずれか１項記載の検出データ処理装置。
【請求項１３】
上記コードワードは、離散コサイン変換領域においてマテリアルアイテムに導入され、当該検出データ処理装置は、
上記ウォータマークが付されたバージョンとオリジナルマテリアルアイテムとを離散コサイン変換領域に変換する離散コサイン変換プロセッサを備え、上記再生プロセッサは、上記オリジナルマテリアルアイテムの離散コサイン変換係数から、上記ウォータマークが付されたバージョンの対応する離散コサイン変換係数を減算することにより、上記再生コードワードを生成することを特徴とする請求項９乃至１２いずれか１項記載の検出データ処理装置。
【請求項１４】
マテリアルアイテムの受信者を特定する受信者特定システムにおいて、
上記受信者を固有に特定するシード値から生成されたコードワードをマテリアルアイテムに導入することにより、ウォータマークが付されたマテリアルアイテムを生成する請求項１乃至６いずれか１項記載の符号化データ処理装置と、
上記マテリアルアイテムにおけるコードワードの有無を検出することにより、所定の誤検出確率で該マテリアルアイテムの受信者を検出する請求項９乃至１３いずれか１項記載の検出データ処理装置とを備える受信者特定システム。
【請求項１５】
オリジナルマテリアルアイテムのコピーに所定のコードワードの組のうちの１つのコードワードを導入することにより、該オリジナルマテリアルアイテムの少なくとも１つのウォ

ータマークが付されたコピーを生成する符号化方法において、
複数のコードワード係数を有するコードワードを生成するステップと、
上記コードワード係数を上記マテリアルアイテムに結合するステップとを有し、
上記コードワードを生成するステップは、
第１の複数のコードワード係数を有する第１のコードワードを生成するステップと、
該第１のコードワードを循環的にシフトして少なくとも１つの他のコードワードを生成するステップとを有する符号化方法。
【請求項１６】
オリジナルマテリアルのコピーの各サンプルに、それぞれ対応する各コードワード係数を結合することにより生成された、オリジナルマテリアルアイテムのウォータマークが付されたバージョン内に存在する１つ以上の所定のコードワードの組を識別する識別方法において、
上記ウォータマークが付されたマテリアルアイテムからコードワードを再生し、再生コードワードを生成するステップと、
所定の閾値を超えるコードワードの相関値から少なくとも１つのコードワードを検出するステップとを有し、
上記複数のコードワードの相関値は、
上記再生コードワードのフーリエ変換値を算出し、
上記コードワードの組の第１のコードワードのフーリエ変換値を算出し、
上記再生コードワードのフーリエ変換値及び上記生成されたコードワードのフーリエ変換値のいずれか一方の複素共役を算出し、
上記再生コードワードの各フーリエ変換サンプルと対応する上記第１のコードワードのフーリエ変換サンプルとを乗算して第１の中間積サンプルを算出し、
上記中間積サンプルを逆変換し、それぞれが上記コードワードの組のうちの１つの相関値を表す相関サンプルを算出することにより求められる識別方法。
【請求項１７】
請求項１乃至６いずれか１項記載の符号化データ処理装置によってコードワードが付加されたマテリアルアイテムを表すデータ信号。
【請求項１８】
請求項１７記載のデータ信号が記録されたデータ媒体。
【請求項１９】
データプロセッサにロードされて、該データプロセッサを請求項１乃至６いずれか１項記載の符号化データ処理装置又は請求項９乃至１３いずれか１項記載の検出データ処理装置として動作させるコンピュータにより実行可能な命令を提供するコンピュータプログラム。
【請求項２０】
データプロセッサにロードされて、該データプロセッサに請求項１５又は１６記載の方法を実行させるコンピュータにより実行可能な命令を提供するコンピュータプログラム。
【請求項２１】
請求項１９又は２０記載のコンピュータプログラムを表す情報信号が記録されているコンピュータにより読取可能な媒体を備えるコンピュータプログラム製品。
【請求項２２】
マテリアルアイテムを表す信号を受信する受信装置であって、請求項１乃至６いずれか１項記載の符号化データ処理装置を備え、受信信号を固有に識別する少なくとも１つのコードワードを該受信信号に結合する受信装置。
【請求項２３】
添付の図面を参照して以下に説明する検出データ処理装置又は符号化データ処理装置。
【請求項２４】
添付の図面を参照して以下に説明する所定のコードワードのうち少なくとも１つのコードワードを識別する識別方法又はオリジナルマテリアルの少なくとも１つのウォータマーク

が付されたコピーを作成する作成方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、マテリアルのバージョンに埋め込まれたコードワードを検出する検出データ処理装置に関する。いくつかの具体例においては、コードワードは、マテリアルアイテムを識別するために使用される。

【０００２】

【従来の技術】

マテリアルを識別するために、マテリアルに情報を埋め込む処理は、ウォータマーキング処理と呼ばれる。

【０００３】

識別コードワードは、マテリアルアイテムのバージョンを識別するために、マテリアルアイテムのバージョンに埋め込まれる。すなわち、ウォータマーキング処理により、マテリアルの特定のバージョンの受信者を特定することができる。ここで、マテリアルの配信者の意向にそぐわない形でマテリアルがコピー又は使用された場合、配信者は、識別コードワードからマテリアルのバージョンを特定し、適切な対策を講ずることができる。

【０００４】

この明細書においては、マテリアルの供給者、所有者、作成者又は配信者の意向にそぐわない形でコピー又は使用されたマテリアルアイテムを、便宜的にマテリアルのオフェンディングアイテム（ｏｆｆｅｎｄｉｎｇ　ｉｔｅｍ）又はオフェンディングマテリアル（ｏｆｆｅｎｄｉｎｇ　ｍａｔｅｒｉａｌ）と呼ぶ。

【０００５】

マテリアルは、ビデオマテリアル、オーディオマテリアル、オーディオ／ビデオマテリアル、ソフトウェアプログラム、デジタル文書及びいかなる種類の情報を含むマテリアル（ｉｎｆｏｒｍａｔｉｏｎ　ｂｅａｒｉｎｇ　ｍａｔｅｒｉａｌ）のいずれであってもよい。

【０００６】

ウォータマークの仕組みを成功させるためには、ユーザが識別コードを除去することが可能な限り困難である必要がある。また、ユーザが識別コードを変更し、マテリアルのオフェンディングアイテムの作成者を他人にみせかけることも可能な限り困難である必要がある。このようなユーザによるコードワードのマスク又はコードワードが他のユーザを示すようにするような改竄は、コルージョンアタック（ｃｏｌｌｕｓｉｏｎ　ａｔｔａｃｋ）と呼ばれる。

【０００７】

【発明が解決しようとする課題】

全てのウォータマークの仕組みにおいて、同じマテリアルのコピーを受け取ったユーザがコルージョンアタックに成功することが困難となるようにする必要がある。したがって、ウォータマークの仕組みは、コルージョンアタックの対象となったウォータマークが付されているマテリアルアイテムを高い確率で特定できるものである必要がある。この特定は、オフェンディングマテリアルから再生されたコードワードを識別することにより実現される。一方、コードワードが存在するのにコードワードが存在しないと判定してしまう確率（見逃し確率：ｆａｌｓｅ　ｎｅｇａｔｉｖｅ　ｐｒｏｂａｂｉｌｉｔｙ）は、低くなくてはならない。更に、実際にはコルージョンアタックに加担していないユーザを誤って不正行為を行ったユーザであると判定してしまう確率（誤検出確率：ｆａｌｓｅ　ｐｏｓｉｔｉｖｅ　ｐｒｏｂａｂｉｌｉｔｙ）は、可能な限り低くしなくてはならない。

【０００８】

米国特許第５６６４０１８号は、マテリアルから複数のコピーに所定数の係数を有するコードワードから作成されたデジタルウォータマークを付すウォータマーキング処理を開示している。ウォータマークが付されるマテリアルアイテムは、例えば画像である。ここで

開示されているウォータマークの埋込を行う装置は、画像を離散コサイン変換（Ｄｉｓｃｒｅｔｅ　Ｃｏｓｉｎｅ　Ｔｒａｎｓｆｏｒｍ：以下、ＤＣＴという。）領域に変換する。デジタルウォータマークは、正規分布を有し、ランダムに分布した係数の組から構成されている。ＤＣＴ領域において、それぞれ各ＤＣＴ係数に対応する各コードワード係数が付加される。これに関連する文献である１９９８年７月２７日、ＭＩＴから発行された、ジェイ・キリアン（Ｊ．Ｋｉｌｉａｎ）、エフ・ティー・レイトン（Ｆ．Ｔ．Ｌｅｉｇｈｔｏｎ）著、「コルージョンアタックに対するデジタルウォータマークの保護（Ｒｅｓｉｓｔａｎｃｅ　ｏｆ　Ｄｉｇｉｔａｌ　Ｗａｔｅｒｍａｒｋｓ　ｔｏ　Ｃｏｌｌｕｓｉｏｎ　Ａｔｔａｃｋｓ）」には、アタックを防ぐためのこのウォータマーキング処理の詳細な数学的解析が開示されている。

【０００９】

【課題を解決するための手段】

本発明に係る符号化データ処理装置は、オリジナルマテリアルアイテムのコピーに所定のコードワードの組のうちの１つのコードワードを導入することにより、該オリジナルマテリアルアイテムの少なくとも１つのウォータマークが付されたコピーを生成する。コードワードは、複数のコードワード係数を有する。符号化データ処理装置は、コードワード係数をマテリアルアイテムに結合する符号化プロセッサを備える。所定のコードワードの組内の複数のコードワードは、第１の複数のコードワード係数を有する第１のコードワードと、この第１のコードワードを循環的にシフトして生成された少なくとも１つの他のコードワードとを含む。

【００１０】

本発明は、米国特許第５６６４０１８号に開示されているような、ランダムに分布した係数を有するコードワードを利用した現実的なウォータマークシステムを提供することを目的とする。現実的に有効なシステムを実現するためには、固有に識別できるコードワードの数は可能な限り大きい方がよい。例えばビデオ機器等の民生用機器や映画館用の映写機等への配信のためには、数百万、好ましくは数千万のコードワードの組を設ける必要がある。ここで、一千万個のコードワードからなるコードワードの組を生成し、生成された各コードワードと再生コードワードとを相関させる処理は、大きな処理負担となる。高性能コンピュータを用いても、このような相関処理は、非現実的な又は少なくともユーザが不便と感じる程の長い時間を要する。本発明の具体例では、一組のコードワードに対する相関の演算を効率的に行うことができる。この具体例では、コードワードの組のうち、少なくとも一部のコードワードは、第１のコードワードを生成し、この第１のコードワードを循環的にシフトして他のコードワードを算出することにより生成される。これにより、組内の全てのコードワードの相関値は、フーリエ変換相関器を用いて算出できる。後述するように、フーリエ変換相関器は、一組の相関値を１回の処理で算出し、演算タスクを実質的に軽減する。

【００１１】

また、本発明に係る検出データ処理装置は、ウォータマークが付されたマテリアルアイテムからコードワードを再生し、再生コードワードを生成する復号プロセッサと、少なくとも１つのコードワードを検出する検出プロセッサとを備える。コードワードは、復元されたコードワードを生成された複数のコードワードのそれぞれに相関させることにより算出された相関値に基づいて検出される。すなわち、相関値が所定の閾値を超える場合、対応するコードワードが検出される。この相関値は、再生コードワードのフーリエ変換値を算出し、コードワードの組の第１のコードワードのフーリエ変換値を算出し、再生コードワードのフーリエ変換値及び生成されたコードワードのフーリエ変換値のいずれか一方の複素共役を算出し、再生コードワードの各フーリエ変換サンプルと対応する第１のコードワードのフーリエ変換サンプルとを乗算して第１の中間積サンプルを算出し、中間積サンプルを逆変換し、それぞれがコードワードの組のうちの１つの相関値を表す相関サンプルを算出することにより求められる。

【００１２】

好適な具体例においては、符号化プロセッサは、順序変更コードに基づいて、上記コードワード係数が結合される順序を変更する。これに対応して、好適な具体例においては、検出データ処理装置は、生成されたコードワード係数又は再生コードワード係数の順序を戻して相関値の算出を行う。第１のコードワードを循環的にシフトすることによりコルージョンアタックが成功する確率が高くなるが、コードワード係数の順序を変更することにより、この確率を低減することができる。

【００１３】

本発明の更なる側面及び特徴は、添付の請求の範囲において定義されている。

【００１４】

【発明の実施の形態】

ウォータマークシステムの概観

以下、本発明の実施の形態をビデオ画像の保護に関連させて説明する。ビデオ画像を配信すべきユーザの数によりコピーの数が決定する。各コピーには、これらのユーザのうちの１人に割り当てられたコピーを識別するための識別コードワード（ｉｄｅｎｔｉｆｉｃａｔｉｏｎ　ｃｏｄｅ　ｗｏｒｄ）が付加される。

【００１５】

ビデオ画像は、デジタルコードワードを埋め込むことにより保護されるマテリアルの一具体例である。コードワードを埋め込むことにより保護されるマテリアルは、ビデオ画像の他に、ソフトウェアプログラム、デジタル文書、音楽、オーディオ信号及び他のいかなる種類の情報を含むマテリアルであってもよい。

【００１６】

図１は、オリジナル画像のコピーに識別コードワードを導入する符号化画像処理装置（ｅｎｃｏｄｉｎｇ　ｉｍａｇｅ　ｐｒｏｃｅｓｓｉｎｇ　ａｐｐａｒａｔｕｓ）の具体的構成を示すブロック図である。オリジナル画像Ｉは、ソースから供給され、フレームメモリ１に保存される。このオリジナル画像は、ウォータマークが付された複数のコピーとして複写される（ｒｅｐｒｏｄｕｃｅ）ものであり、各コピーには、固有の識別コードワードが付される。オリジナル画像は、ＤＣＴプロセッサ２に供給され、ＤＣＴプロセッサ２は、オリジナル画像を８×８の画素ブロックに分割し、８×８の各画素ブロックにＤＣＴ処理を施す。これにより、ＤＣＴプロセッサ２は、ＤＣＴ変換画像Ｖを生成する。

【００１７】

以下の説明において、「サンプル」という用語は、画像（又は、実際には他の種類のマテリアルであってもよい。）を構成する離散サンプルを指すものとする。サンプルは、画素からも複写することができる画像の輝度サンプルであってもよい。したがって、サンプルという用語と画素という用語は、状況によっては交換可能である場合もある。

【００１８】

ＤＣＴ画像Ｖは、符号化プロセッサ（以下、エンコーダともいう。）４に供給される。符号化プロセッサ４には、識別コードワード生成器８から識別コードワードも供給されている。

【００１９】

識別コードワード生成器８には、複数のシード値（ｓｅｅｄ）が供給される。各シード値は、それぞれ対応する識別コードワードの１つを生成するために使用される。生成された各識別コードワードは、オリジナル画像のコピーに埋め込まれ、これによりウォータマークが付された画像が生成される。識別コードワード生成器８は、疑似乱数生成器を備える。疑似乱数生成器は、特定の識別コードワードを形成するためのコードワード係数を生成する。好ましい具体例においては、コードワード係数は、正規分布に基づいて生成される。なお、これに代えて、コードワード係数は、疑似乱数生成器を初期化するために用いるシード値に基づいて、予め定めてもよい。したがって、各識別コードワードには、対応するシード値が存在し、各シード値は、メモリ１２に記憶されている。すなわち、識別コードワードX^{1}を生成するために、シード値$seed_1$をメモリ１２から読み出し、このシード値$seed_1$を用いて、識別コードワード生成器８内の疑似乱数生成器を初期化する

【００２０】
以下の説明では、オリジナル画像のＤＣＴバージョンをＶと表す。ここで、
$V = \{v_i\} = \{v_1, v_2, v_3, v_4, \cdots, v_N\}$
であり、v_iは、画像のＤＣＴ係数である。他の具体例においては、v_iは、画像のサンプル値であり、空間領域における画像のサンプル値又は他の領域における画像のサンプル値を表すものであってもよい。
【００２１】
各識別コードワードX^iは、以下のように、ｎ個のコードワード係数から構成されている。
$X^i = \{x^i_j\} = \{x^i_1, x^i_2, x^i_3, x^i_4, \cdots, x^i_n\}$
コードワード係数の数ｎは、オリジナル画像Ｖのサンプル数に対応する。なお、係数の数は異なるものであってもよく、この数は、特定のアプリケーションに応じて決定してもよい。
【００２２】
そして、ｉ番目の識別コードワードX^iを構成するコードワード係数のベクトルは、チャンネル１４を介してエンコーダ４に供給される。エンコーダ４は、画像Ｖに識別コードワードX^iを付加することにより、ウォータマークが付された画像W_iを生成する。実際には、以下の式に示すように、画像の各係数に各コードワード係数を加えることにより、ウォータマークが付された画像W_iが生成される。
$W_i = V + X^i$
$W_i = v_1 + x^i_1, v_2 + x^i_2, v_3 + x^i_3, v_4 + x^i_4, \cdots, v_n + x^i_n$
図１に示すように、ウォータマークが付された画像W_iは、エンコーダ４により生成された画像を逆ＤＣＴ変換する逆ＤＣＴプロセッサ１８によって、逆ＤＣＴ変換された後、この画像処理装置から出力される。
【００２３】
したがって、図１に示すように、エンコーダ４からは、ウォータマークが付された画像の組が出力される。データワードを最大２０ビットとすると、一千万個の識別コードワードの１つを選択することができ、オリジナル画像に対して、一千万個のウォータマークが付されたバージョンW_iを生成することができる。
【００２４】
この識別コードワードにより、画像Ｉのウォータマークが付されたコピーW_iを個別に識別することができるが、他の具体例においては、上述の２０ビットにより、画像内でデータを送ることができる。したがって、以下に説明するように、識別コードワードを選択するために使用される２０ビットは、画像Ｖ内でデータを送るための２０ビットのペイロードを提供する。
【００２５】
図１に示す、ウォータマークが付された画像を生成する符号化画像処理装置は、本発明が適用される様々な異なるシナリオにおいて、様々な製品に組み込まれる。例えば、符号化画像処理装置をウェブサイト又はウェブサーバに接続して、ウォータマークが付された画像をダウンロードすることができる。画像のコピーをダウンロードする前に、ダウンロードされる画像には固有のコードワードが導入され、この固有のコードワードにより、ダウンロードされた画像の受信者を後に検出することができる。
【００２６】
他の適用例では、符号化画像処理装置は、デジタル映写機（ｄｉｇｉｔａｌ　ｃｉｎｅｍａ　ｐｒｏｊｅｃｔｏｒ）の一部として組み込まれ、識別コードワードは、例えば映画館において、映画を映写する際に、映像に付加される。この識別コードワードにより、映画が映写された映写機及び映画館を特定することができる。したがって、映写機から映写された映像を撮影して得られた海賊版コピーに含まれる識別コードワードにより、その海賊

版コピーが作成された映写機及び映画館を特定することができる。一方、ウォータマークが付された画像は、写真又は印刷物として複写されてもよく、複写された写真又は印刷物のコピーを作成及び配布してもよい。図１においては、符号化画像処理装置によって生成されるウォータマークが付された画像の配信先は、雲形の枠で表現された配信１９で示されている。

【００２７】

検出プロセッサ

図２は、ウォータマークが付されたオフェンディング画像（ｏｆｆｅｎｄｉｎｇ ｍａｒｋｅｄｉｍａｇｅ）内に埋め込まれている１つ以上のコードワードを検出する検出画像処理装置（ｄｅｔｅｃｔｉｎｇ ｉｍａｇｅ ｐｒｏｃｅｓｓｉｎｇ ａｐｐａｒａｔｕｓ）の構成を示すブロック図である。包括的にいえば、図２に示す検出画像処理装置は、画像のオフェンディング、すなわちコピー内に存在する１つ以上のコードワードを識別する機能を有している。

【００２８】

ウォータマークが付された画像のオフェンディングバージョンW’は、データ源から供給され、フレームメモリ２０に保存される。この検出画像処理装置における検出処理は、画像のオリジナルバージョンを必要とするため、フレームメモリ２４には、画像のオリジナルバージョンが保存されている。ウォータマークが付された画像のオフェンディングバージョンW’及び画像のオリジナルバージョンは、それぞれ個別の接続チャンネル２６、２８を介して、登録プロセッサ（ｒｅｇｉｓｔｒａｔｉｏｎ ｐｒｏｃｅｓｓｏｒ）３０に供給される。

【００２９】

上述のように、画像のオフェンディングバージョンW’は、ウォータマークが付された画像W_Iの一部を撮影又は複写することにより生成された可能性がある。そこで、識別コードワードの検出率を高めるために、登録プロセッサ３０は、それぞれフレームメモリ２０、２４に保存されているオフェンディング画像と画像のオリジナルバージョンとを実質的に揃える（ａｌｉｇｎ）。この目的は、オリジナル画像のサンプルＩと、ウォータマークが付され、コードワード係数が付加されている対応する画像W_Iのサンプルとの対応関係を調べることである。

【００３０】

この登録処理を図３を用いて説明する。図３は、オリジナル画像Ｉとウォータマークが付された画像のオフェンディングバージョンW’とを比較して示している。図３に示すように、ウォータマークが付された画像のオフェンディングバージョンW’は、オリジナル画像に対してオフセットを有しており、このオフセットは、ウォータマークが付された画像のオフェンディングバージョンが生成されたカメラの相対的な視野に起因する可能性がある。

【００３１】

コードワード係数の表現を再生するために、ウォータマークが付された画像のオフェンディングバージョンW’からオリジナル画像の正しいサンプルを減算する必要がある。この処理のために、２つの画像が揃えられる。図３に示すように、登録された画像W”は、オリジナル画像には存在しない部分を含む周辺領域（ｐｅｒｉｐｈｅｒａｌ ａｒｅａ）ＰＡを有している。

【００３２】

他の具体例では、例えばインターネットからオフェンディングバージョンがダウンロードされた場合等、オフェンディング画像W’と既にオリジナル画像のバージョンＩとの対応関係が明かであることがあり、このような場合、登録プロセッサ３０を使用する必要はない。そこで、この検出画像処理装置は、ウォータマークが付された画像を再生プロセッサ４０に直接供給するための代替的なチャンネル３２を備えている。

【００３３】

登録された画像W”は、再生プロセッサ４０に供給される。再生プロセッサ４０には、第

２のチャンネル４４を介して、オリジナル画像Ｉのコピーも供給される。登録された画像Ｗ”及びオリジナル画像Ｉは、ＤＣＴプロセッサ４６によって、ＤＣＴ領域に変換される。次に、以下の式に示すように、オリジナル画像のＤＣＴ領域のサンプルＶからウォータマークが付された画像のＤＣＴ領域のサンプルＶ’を減算することにより、推定コードワードＸ’が算出される。

$X' = V' - V$

$= v'_1 - v_1, v'_2 - v_2, v'_3 - v_3, v'_4 - v_4, \cdots, v'_n - v_n$

$= x'_1, x'_2, x'_3, x'_4, \cdots, x'_n$

したがって、再生プロセッサ４０は、接続チャンネル５０を介して、識別すべきコードワードの係数の推定値を出力する。再生されたコードワードＸ’は、相関器５２の第１の入力端子に供給される。相関器５２の第２の入力端子には、コードワード生成器５４によって生成されたコードワードX^iが供給されている。コードワード生成器５４は、上述の識別コードワード生成器８と同様に、メモリ５８から読み出したコードワードを固有に識別する所定のシード値を用いて全ての可能なコードワードの組を生成する。

【００３４】

相関器５２は、ｎ個の類似値ｓｉｍ（ｉ）を生成する。一具体例においては、類似値ｓｉｍ（ｉ）は、以下の式に基づく相関を求めることにより算出される。

【００３５】

【数１】

$$sim(i)=\frac{X^i * X'}{\sqrt{X^i * X'}}=\frac{x^i_1 * x'_1+x^i_2 * x'_2+x^i_3 * x'_3+\ldots+x^i_n * x'_n}{\sqrt{x^i_1 * x'_1+x^i_2 * x'_2+x^i_3 * x'_3+\ldots+x^i_n * x'_n}}$$

【００３６】

ｎ個の類似値ｓｉｍ（ｉ）のそれぞれは、検出器６０に供給される。そして、検出器６０は、ｎ個の可能なコードワードのそれぞれに対する類似値ｓｉｍ（ｉ）を分析する。相関器５２によって生成される類似値ｓｉｍ（ｉ）の具体例と、可能な各コードワードの閾値ＴＨとの関係を図４に示す。図４に示すように、２つのコードワード２００１、１２３４５が閾値ＴＨを超えている。このため、検出器６０は、コードワード２００１及びコードワード１２３４５に対応するウォータマークが付された画像のバージョンからオフェンディング画像が作成されたと判定する。したがって、この具体例においては、一千万である母集団の大きさにより決定される誤検出確率（ｆａｌｓｅ　ｐｏｓｉｔｉｖｅ　ｐｒｏｂａｂｉｌｉｔｙ）と、ウォータマーク強度（ｗａｔｅｒｍａｒｋｉｎｇ　ｓｔｒｅｎｇｔｈ）とに基づいて、誤検出確率を保証する閾値ＴＨの高さを設定することができる。図４に示す具体例では、相関器５２によって生成された類似値が閾値を超えている場合、この誤検出確率をもって、このウォータマークが付された画像の受信者が不正行為を行い、ウォータマークが付された画像のオフェンディングバージョンW^iの作成に関与したと判断される。

【００３７】

以下、図１及び図２に示すウォータマークシステムの特徴及び利点を説明する。

【００３８】

登録

ウォータマークが付された画像のオフェンディングバージョンと、オリジナル画像のコピーとを揃える処理は、オリジナル画像のサンプルと、ウォータマークが付された画像のサンプルとの相関を調べる処理を含む。この相関処理は、画像の各サンプルを異なるシフト量でシフトさせて実行される。この処理を図５を用いて説明する。図５Ａは、オリジナル画像の離散サンプルを示し、図５Ｂは、ウォータマークが付されたオフェンディング画像Ｗ’の離散サンプルを示している。図５Ａ及び図５Ｂに示すように、各サンプル間の時間

差は、サンプリングレートにより定まるｄｔである。これらの画像の各サンプルの組をシフトし、離散サンプルを相関させた結果を図５Ｃに示す。

【００３９】

図５Ｃに示すように、第６サンプルと第７サンプルの間で相関ピークが最高になっている。そこで、ウォータマークが付されたオフェンディング画像は、オリジナル画像に対してこの量だけシフトされて登録される。

【００４０】

フーリエ復号

図１及び図２を参照して上述したウォータマークシステムは、オリジナル画像に対して一千万個のウォータマークが付されたバージョンを作成することができる。これは、２０ビットのウォータマーク値を用いることにより実現される。ここで、上述のように、複数のコードワードのうち、ウォータマークが付されたオフェンディング画像内のコードワードの存在を検出するためには、その画像から再生されたコードワードと、一千万個の可能な各コードワードとの相関を調べる必要がある。このような演算タスクは大きな処理負担となる。

【００４１】

本発明に基づく相関器は、この演算処理の負担を軽減し、したがってウォータマークが付されたオフェンディング画像内のコードワードを検出するために必要な時間を短縮する。本発明に基づくこの相関器を図６に示す。図６に示す相関器は、上述した相関値の総和の算出に対する代替的で有効な手法を提供する。すなわち、この具体例では、相関値の総和は、以下の式に基づいて算出される。

$F^{-1}[F(X')F(x^{(1)})^*]$

ここで、Ｆ（Ａ）はＡのフーリエ変換を表し、F^{-1}（Ａ）はＡの逆フーリエ変換を表す。

【００４２】

図６に示す相関器５２は、第１のフーリエ変換プロセッサ１００と、第２のフーリエ変換プロセッサ１０２とを備える。第１及び第２のフーリエ変換プロセッサ１００、１０２は、高速フーリエ変換アルゴリズムを用いて実現してもよい。第２のフーリエ変換プロセッサ１０２は、生成されたコードワードのフーリエ変換値の複素共役X^1も算出する。再生コードワードのフーリエ変換値Ｘ’と、生成されたコードワードのフーリエ変換の複素共役X^1は、それぞれ乗算器１１０の第１及び第２の入力端子に供給される。乗算器１１０は、フーリエ変換プロセッサ１００、１０２からの各サンプルを乗算し、この結果を逆フーリエ変換プロセッサ１１２に供給する。この相関器５２からは、乗算された信号サンプルの逆フーリエ変換値が出力される。

【００４３】

このように、図６に示す相関器５２では、生成されたｎ個のコードワードX^iと再生コードワードＸ’との相関を算出するために必要な時間が短縮される。これは、フーリエ変換プロセッサ１００、１０２、１１２を例えば市販されている特定用途向け集積回路（ａｐｐｌｉｃａｔｉｏｎ ｓｐｅｃｉｆｉｃ ｉｎｔｅｇｒａｔｅｄ ｃｉｒｃｕｉｔ：ＡＳＩＣ）等の高速フーリエ変換集積回路により構成できるためである。更に、相関器５２から出力される逆フーリエ変換値は、ｎ個の相関値の総和に対応するｎ個の類似値ｓｉｍ（ｉ）を提供する。ここで、図６に示す相関器５２の特性を利用するために、コードワードは、乱数生成器に供給される特定のシード値を用いて、生成された１つのコードワード$X^{(1)}$を循環的にシフトすることにより生成されている。以下、このコードワードの生成について説明する。後述するように、第１のコードワード$X^{(1)}$は、コードワード生成器８によって疑似ランダム的に生成された数値に対応する値x_1～x_nとして表される。一方、第２のコードワード$X^{(2)}$は、第１のコードワード$X^{(1)}$に対する循環的シフトを実行することにより生成される。更に、以下に示すように、この他のコードワードは、ｎ番目のコードワードがｎ－１の位置にシフトされるまで、第１のコードワード$X^{(1)}$を循環的にシフトすることにより生成される。

$X^{(1)} = (x_1, x_2, x_3, x_4 \cdots, x_{n-1}, x_n)$
$X^{(2)} = (x_2, x_3, x_4 \cdots, x_{n-1}, x_n, x_1)$
$X^{(3)} = (x_3, x_4 \cdots, x_{n-1}, x_n, x_1, x_2)$
・・・
$X^{(n)} = (x_n, x_1, x_2, x_3, x_4 \cdots, x_{n-2}, x_{n-1})$

このコードワードの組を用いて、符号化画像プロセッサによって生成されるコードワードの組の一部又は全部を構成することにより、フーリエ変換を行う相関器５２は、一回の処理でｎ個の全てのコードワードに関する全ての類似値を算出することができる。したがって、上述のように、オリジナルコードワードに対する１からｎまでの対応するシフトにより、ｎ個の類似値の総和ｓｉｍ（ｉ）が生成され、図４に示すように、少なくとも１つのコードワードについて、大きな類似値の総和ｓｉｍ（ｉ）が生成される。このように、相関器５２は、第１のコードワード$X^{(1)}$に対応する１つの生成されたコードワードのみを受け取って、図４に示すようにｎ個のコードワードの組に関する類似値を算出することができる。

【００４４】

以上の説明から明かなように、コードワードに含まれるサンプルがＮ個であれば、可能な循環シフトはＮ個のみである。したがって、必要なコードワードの母集団ｐがＮより大きければ、複数の基礎となるウォータマークが必要となる。各基礎となるウォータマークは、循環的にシフトされ、Ｎ個の固有なコードワードが生成される。

【００４５】

ウォータマークが付された画像が、例えばビデオシーケンス等の複数の画像の１つを構成する場合、各画像には同じコードワードを付すことができる。したがって、図６に示すフーリエ変換相関器を用いて、１つの判定中のコードワード（ｓｕｓｐｅｃｔｅｄ　ｃｏｄｅ　ｗｏｒｄ）が特定されると、上述のように、完全な相関値の総和ｓｉｍ（ｉ）を用いても、後続する相関値を算出することができる。ここで、判定中のコードワードは既に特定されているため、相関処理は、図６に示すフーリエ変換相関器によって特定されたコードワードに対してのみ行えばよい。

【００４６】

また、生成された第１のコードワードX^1のフーリエ変換値の複素共役を算出する代わりに、再生コードワードのフーリエ変換値の複素共役を算出してもよい。この処理は、以下に示すフーリエ変換相関器による処理の第２の変形例として表される。

$F^{-1}[F(X') * F(x^{(1)})]$

このように、再生コードワードのフーリエ変換値の複素共役及び生成されたコードワードのフーリエ変換値のいずれかがフーリエ変換プロセッサ１００、１０２のいずれかによって算出される。

【００４７】

コードワードの秘密の順序変更

第１のコードワードX^1を循環的にシフトさせてコードワードを生成する手法では、ウォータマークのセキュリティが低下するという問題がある。これは、コルージョンアタックにおいては、ウォータマークが付された２つの画像が比較されるからである。各画像に対し、同じコードワードを循環的にシフトさせて生成した同じコードワードの２つのバージョンであるコードワードを付加した場合、コルージョンアタックを試みる者は、ウォータマークが付された２マテリアル間の相異を特定し、したがってコードワードを特定しやすくなる。コルージョンアタックを試みる者がコードワードを特定できると、この者は、ウォータマークを除去し、又はウォータマークを改竄して他者を装うことができるようになる。

【００４８】

このようなコルージョンアタックを防止するために、この具体例では、秘密の順序変更コード（ｓｅｃｒｅｔ　ｐｅｒｍｕｔａｔｉｏｎ　ｃｏｄｅ）πに基づいて、循環的にシフトされた各コードワードの各コードワード係数の順序をランダムに変更する。コードワー

ド係数の順序変更は、ウォータマークが付された画像の受信者に対して秘密にされる。これにより、コルージョンアタックを試みる者がウォータマークが付された２つの画像間の相関を特定することが困難になり、コルージョンアタックが成功する可能性が低下する。

【００４９】

検出データプロセッサにおいては、秘密の順序入替コードπは既知である。検出データプロセッサにおいては、コードワード生成器又は復元プロセッサ４０が生成したコードワード係数又は再生コードワード係数に対して逆の順序入替π^{-}を実行した後、相関処理を行う。図１に示す符号化データプロセッサ及び図２に示す検出データプロセッサの動作をそれぞれ図７及び図８に示す。

【００５０】

コードワード生成

コードワードを生成するために使用される乱数のシード値をソース画像サンプルから生成することにより、図１及び図２に示す本発明の具体例の性能を更に高めることができる。この処理は、ウォータマークを付すべき画像のＤＣＴ係数を分析し、これらのＤＣＴ係数から、コードワードを生成するために使用するシード値を生成することにより実現される。この処理には、例えば、当業者にとって周知の「セキュアハッシュアルゴリズム１（ｓｅｃｕｒｅ ｈａｓｈｉｎｇ ａｌｇｏｒｉｔｈｍ １：ｓｈａ－１）」を用いることができる。このアルゴリズムは、ＡＮＳＩ規格（ＡＮＳＩ ｘ９．３０－２）に規定されている。このアルゴリズムは、エー・ジェイ・メネゼス（Ａ．Ｊ．Ｍｅｎｅｚｅｓ）著「応用暗号学ハンドブック（Ｈａｎｄｂｏｏｋ ｏｆ ａｐｐｌｉｅｄ ｃｒｙｐｔｏｇｒａｐｈｙ）」にも開示されている。これにより、符号化画像処理装置及び検出画像処理装置は、ＤＣＴ係数から乱数のシード値を生成及び判定することができる。

【００５１】

他の適用例

ウォータマークシステムの符号化データ処理装置は、上述した映写機及びウェブサーバに加えて、他の用途にも適用することができる。例えば、本発明は、通信装置から信号を受信し、この受信した信号にコードワードを導入することにより情報にウォータマークを付す受信機／デコーダにも適用することができる。例えば、セットトップボックスは、放送の「ヘッドエンド」機器又はマルチキャスト機器からテレビジョン及びビデオ信号を受信する。このような適用例では、符号化データ処理装置は、セットトップボックスの一部を構成し、信号を受信及びデコードする際にビデオ信号にウォータマークコードワードを導入する。一具体例においては、このウォータマークコードワードは、ビデオ信号を受信及びデコードしたセットトップボックスを固有に特定する。

【００５２】

更に、本発明は、衛星からデジタル映画データ（ｄｉｇｉｔａｌ ｃｉｎｅｍａ ｆｉｌｍ）を受信するデジタル映画受信機にも適用することができる。このデジタル映画受信機は、デジタル映画を表す信号を受信し、この信号をデコードしてデジタル映画を再生する。この受信機は、デコードされた映画信号にウォータマークコードワードを導入する符号化データ処理装置を備える。ウォータマークコードワードは、例えば、デジタル映画データを受信したデジタル映画受信機を固有に特定する。

【００５３】

更に、本発明は、メモリ及びメモリコントローラを備えるデジタルカメラ又はカムコーダ等にも適用することができる。この適用例では、本発明に係る符号化データ処理装置は、メモリに記憶されているウォータマークコードワードをデジタルカメラ等によって撮影されたビデオ信号に導入する。この適用例においては、コードワードは予めメモリに記憶されており、したがって、符号化データ処理装置は、コードワード生成器を備えていない。メモリに記憶されているコードワードは、メモリコントローラの制御の下、ビデオ信号に埋め込まれ、これによりビデオ信号を固有に又は疑似固有的（ｑｕａｓｉ－ｕｎｉｑｕｅｌｙ）に特定する。

【００５４】

更なる具体例においては、本発明に基づく符号化データ処理装置は、連続的な画像又は動画を構成する複数の異なるデジタル画像のフレームのそれぞれに一連のウォータマークコードワードを個別に埋め込む。これらのコードワードは、互いに関連性を有していてもよく、これらのコードワードにより、各フレームに対応する画像を個別に識別することができるようになる。

【００５５】

本発明の更なる様々な側面及び特徴は、添付の請求の範囲において定義されている。この請求の範囲から逸脱することなく、上述した実施の形態を様々に変更することができる。

【図面の簡単な説明】

【図１】符号化画像処理装置の構成を示すブロック図である。

【図２】検出画像処理装置の構成を示すブロック図である。

【図３】図３Ａはオリジナル画像を示し、図３Ｂはウォータマークが付された画像を示し、図３Ｃは登録された画像を示す図である。

【図４】Ｎ個のコードワードの組の各コードワードに関する相関結果の具体例を示すグラフ図である。

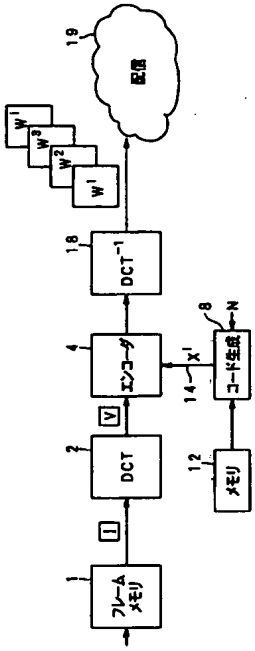
【図５】図５Ａはオリジナル画像Ｉのサンプルに対応するグラフ図であり、図５Ｂはウォータマークが付された画像Ｗ’に対応するグラフ図であり、図５Ｃはオリジナル画像とウォータマークが付された画像との離散サンプルシフト毎の相関結果を示すグラフ図である。

【図６】図２に示す検出データプロセッサの一部である相関器の構成を示すブロック図である。

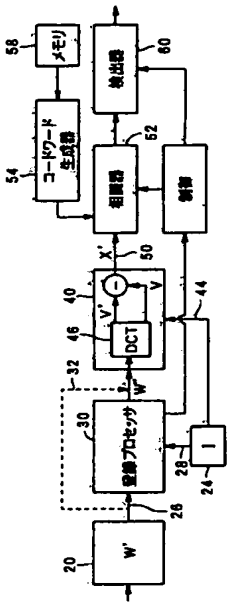
【図７】符号化画像データ処理装置によってウォータマークが付された画像を作成する手順を示すフローチャートである。

【図８】図２に示す検出データプロセッサによって、受信したウォータマークが付された画像からウォータマークを特定する処理を示すフローチャートである。

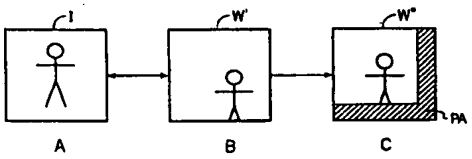
【図１】



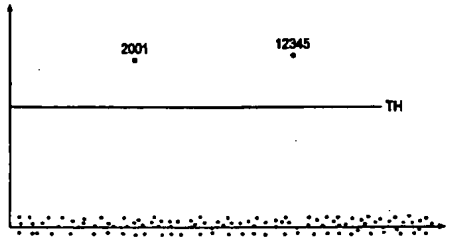
【図２】



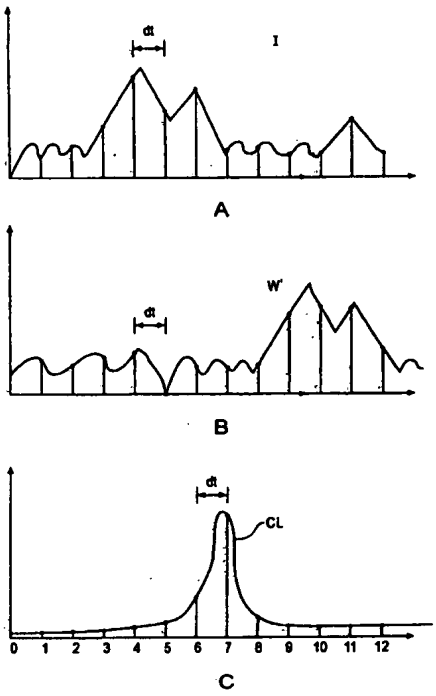
【図３】


I
W'
W*
PA
A
B
C

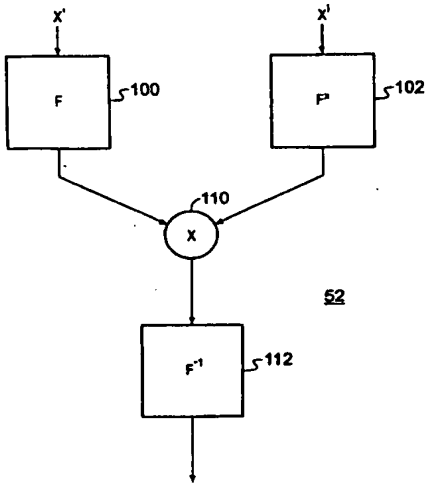
【図４】


2001
12345
TH

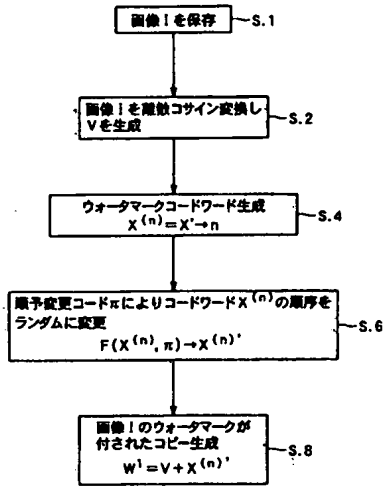
【図５】


dt
I
A
W'
dt
B
dt
CL
0 1 2 3 4 5 6 7 8 9 10 11 12
C

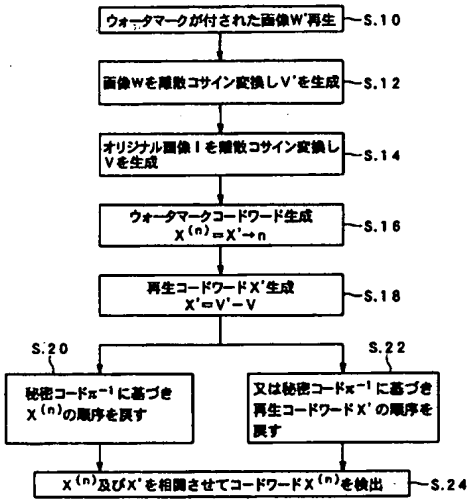
【図６】


X'
X'
F
100
F*
102
110
X
52
F-1
112

【図７】


画像Ｉを保存
S.1
画像Ｉを離散コサイン変換しVを生成
S.2
ウォータマークコードワード生成
X(n)=X'→n
S.4
順予変更コードπによりコードワードX(n)の順序をランダムに変更
F(X(n),π)→X(n)'
S.6
画像Ｉのウォータマークが付されたコピー生成
W'=V+X(n)'
S.8

【図８】


ウォータマークが付された画像W'再生
S.10
画像Wを離散コサイン変換しV'を生成
S.12
オリジナル画像Iを離散コサイン変換しVを生成
S.14
ウォータマークコードワード生成
$X^{(n)} \Rightarrow X' \rightarrow n$
S.16
再生コードワードX'生成
$X' \Rightarrow V' - V$
S.18
S.20
秘密コードπ^{-1}に基づき$X^{(n)}$の順序を戻す
S.22
又は秘密コードπ^{-1}に基づき再生コードワードX'の順序を戻す
$X^{(n)}$及びX'を相関させてコードワード$X^{(n)}$を検出
S.24

フロントページの続き

(51)Int.Cl.[7]	F I	テーマコード(参考)
	H04N 5/91 P	

(72)発明者 ペリー ジェイソン チャールズ
イギリス国 ＫＴ１３ ０ＸＷ サリー ウェイブリッジ ブルックランズ ザ ハイツ（番地なし） ソニー ユナイテッド キングダム リミテッド内
(72)発明者 タプソン ダニエル ワレン
イギリス国 ＫＴ１３ ０ＸＷ サリー ウェイブリッジ ブルックランズ ザ ハイツ（番地なし） ソニー ユナイテッド キングダム リミテッド内

Ｆターム(参考) 5B057 AA11 CA12 CA16 CB12 CB16 CC01 CE08 CH07 CH08
5C053 FA13 GB06 GB21 LA06 LA11
5C076 AA14 BA06
5J104 AA13 AA14 NA13 NA15 NA23

【外国語明細書】

1 Title of Invention

DATA PROCESSING APPARATUS AND METHOD

2 Claims

1. An encoding data processing apparatus for generating at least one marked copy of an original item of material by introducing one of a predetermined set of code words into a copy of said material item, said apparatus comprising

a code word generator operable to provide said code word comprising a plurality of code word coefficients, and

an encoding processor operable to combine the code word coefficients with said material item, wherein

said plurality of code words of said set includes a first code word having a first plurality of code word coefficients, and at least one other code word generated from a cyclic shift of said first code word.

2. An encoding data processing apparatus as claimed in Claim 1, wherein said code word generator includes a pseudo-random number generator operable to generate a pseudo-random numbers from which said code word coefficients are derived.

3. An encoding data processing apparatus as claimed in Claims 1 or 2, wherein said pseudo-random numbers are generated from a seed value for initialising said pseudo-random number generator, which uniquely defines said first code word.

4. An encoding data processing apparatus as claimed in any preceding Claim, wherein said code word generator is operable to generate said seed value from the samples of said material item.

5. An encoding processor as claimed in any preceding Claim, wherein said encoding processor is operable to permute the order in which said code word coefficients are combined with the material in accordance with a permutation code.

6. An encoding data processing apparatus as claimed in any preceding Claim, comprising

a discrete cosine transform processor operable to transform said material item into the discrete cosine transform domain, said material item in said discrete cosine transform domain being represented as a plurality of discrete cosine transform coefficients, wherein said encoding processor is operable to combine said code word with said material item by adding each of said code word coefficients to a corresponding one of said discrete cosine transform coefficients, and

an inverse discrete cosine transform processor operable to form said marked copy of said material item by performing an inverse discrete cosine transform on said discrete cosine transformed image to which said code word has been added by said encoding processor.

7. A cinema projector including an encoding data processing apparatus according to any of Claims 1 to 6, wherein said data processing apparatus is operable to receive at least one of audio signals and image signals before reproduction, and to introduce a code word into said at least one of audio signals and image signals before reproduction.

8. A web server operable to provide material items for downloading via the Internet, said web server including an encoding data processing apparatus according to any of Claims 1 to 6, wherein said data processing apparatus is operable to receive material items and to introduce a code word into said material items before said material items are downloaded.

9. A detecting data processing apparatus operable to identify at least one of a plurality of code words present in a marked version of a material item, said marked version having been formed by combining each of a plurality of samples of an original version of said material with one of a corresponding plurality of code word coefficients, said plurality of code words being formed from a first code word having a plurality of predetermined pseudo-randomly distributed coefficients and by forming at least one other of said plurality of code words by cyclically shifting said first code word, said apparatus comprising

a decoding processor operable to generate a recovered code word from said marked material item, and

a detection processor operable to detect said at least one code word from the correlation value for the code word exceeding a predetermined threshold, wherein said correlation value is formed for a plurality of said code words by

forming a Fourier transform of the recovered code word,

forming a Fourier transform of the first code word of said set,

forming the complex conjugate of one of the Fourier transform of the recovered code word and the Fourier transform of the regenerated code word,

forming intermediate product samples by multiplying each of said Fourier transform samples of said recovered code word and the corresponding Fourier transform samples of said first code word,

forming correlation samples by forming an inverse transform of said intermediate product samples, each of said correlation value samples providing the correlation value for one of said set of code words.

10. A detecting data processing apparatus as claimed in Claim 9, wherein said decoding processor is operable to generate said recovered code word by subtracting corresponding samples of said original material version from said samples of said marked material version, and to generate, for each of said plurality of code words a correlation sum by correlating the recovered code word with each of the plurality of code words.

11. A detecting data processing apparatus as claimed in Claim 9 or 10, comprising

a registering processor operable to associate samples of said marked version of said material item with corresponding samples from said original material item to which corresponding code word coefficients may have been added.

12. A detecting data processing apparatus as claimed in Claim 9, 10 or 11, wherein said correlation processor includes a code word generator operable to generate said seed value from the samples of said marked material item.

13. A detecting data processing apparatus as claimed in any of Claims 9 to 12, wherein said code word has been introduced into said material item in the discrete cosine transform domain, said apparatus comprising

a discrete cosine transform processor operable to transform said marked material item and said original material item into the discrete cosine transform domain, wherein said recovery processor is operable to generate said recovered code word by subtracting corresponding discrete cosine transform coefficients of said original material version from discrete cosine transform coefficients of said marked material version.

14. A system for identifying the recipient of a material item, said system comprising

an encoding data processor according to any of Claims 1 to 6, operable to generate said marked material item by introducing a code word generated from a seed uniquely identifying said recipient, and

a detecting data processor according to any of Claims 9 to 13, operable to detect with a predetermined false positive probability the recipient by detecting the presence or absence of the code word in said material.

15. A method of generating at least one marked version of an original item of material by introducing one of a predetermined set of code words into a copy of said original material item, said method comprising,

providing said code word with a plurality of code word coefficients, and

combining the code word coefficients with said material, wherein said providing said code word comprises

generating a first code word having a plurality of coefficients, and

generating at least one other of said plurality of code words from a cyclic shift of said first code word.

16. A method of identifying one or more of a predetermined set of code words present in a marked version of an original material item, said marked version

having been formed by combining each of a plurality of samples of a copy of said original material item with one of a corresponding plurality of code word coefficients, said method comprising

generating a recovered code word from said marked material item, and

detecting said at least one code word from the correlation value of the recovered code word with a regenerated code word exceeding a predetermined threshold, wherein said correlation value is formed for a plurality of said code words by

forming a Fourier transform of the recovered code word,

forming a Fourier transform of the first code word of said set,

forming the complex conjugate of one of the Fourier transform of the recovered code word and the Fourier transform of the regenerated code word,

forming intermediate product samples by multiplying each of said Fourier transform samples of said recovered code word and the corresponding Fourier transform samples of said first code word,

forming correlation samples by forming an inverse transform of said intermediate product samples, each of said correlation value samples providing the correlation value for one of said set of code words.

17. A data signal representing a material item to which a code word has been added by the data processing apparatus according to any of Claims 1 to 6.

18. A data carrier having recorded thereon a data signal according to Claim 17.

19. A computer program providing computer executable instructions, which when loaded onto a data processor configures the data processor to operate as the encoding data processing apparatus according to any of Claims 1 to 6 or the detecting data processor according to any of Claims 9 to 13.

20. A computer program providing computer executable instructions, which when loaded on to a data processor causes the data processor to perform the method according to Claim 15 or 16.

21. A computer program product having a computer readable medium having recorded thereon information signals representative of the computer program claimed in any of Claims 19 or 20.

22. A receiver operable to receive signals representative of material items, comprising

an encoding data processing apparatus according to Claims 1 to 6, operable to combine at least one code word with the received signals, said code word being provided to identify uniquely said received signals.

23. A detecting or an encoding data processing apparatus as herein before described with reference to the accompanying drawings.

24. A method of identifying at least one of a predetermined set of code words or a method of generating at least one marked copy of an original item of material as herein before described with reference to the accompanying drawings.

3 Detailed Description of Invention

Field of Invention

The present invention relates to encoding data processing apparatus and methods, which are arranged to embed code words into versions of material items. In some applications the code words are used to uniquely identify the material items.

Correspondingly, the present invention also relates to data processing apparatus and methods operable to detect one or more code words, which may be present in a material item.

Background of the Invention

A process in which information is embedded in material for the purpose of identifying the material is referred to as watermarking.

Identification code words are applied to versions of material items for the purpose of identifying the version of the material item. Watermarking can provide, therefore, a facility for identifying a recipient of a particular version of the material. As such, if the material is copied or used in a way which is inconsistent with the wishes of the distributor of the material, the distributor can identify the material version from the identification code word and take appropriate action.

In this description, an item of material, which is copied or used in a way, which is inconsistent with the wishes of the originator, owner, creator or distributor of the material, will be referred to for convenience as an offending item of material or offending material.

The material could be any of video, audio, audio/video material, software programs, digital documents or any type of information bearing material.

For a watermarking scheme to be successful, it should be as difficult as possible for the users to collude in order to mask or remove the identification code words. It should also be as difficult as possible for users to collude to alter the identification code word to the effect that one of the other users is falsely indicated as the perpetrator of an offending item of material. Such an attempt by users to collude to either mask the code word or alter the code word to indicate another user is known as a collusion attack.

Any watermarking scheme should be arranged to make it difficult for users receiving copies of the same material to launch a successful collusion attack. A watermarking scheme should therefore with high probability identify a marked material item, which has been the subject of a collusion attack. This is achieved by identifying a code word recovered from the offending material. Conversely, there should be a low probability of not detecting a code word when a code word is present (false negative probability). In addition the probability of falsely detecting a user as guilty of taking part in a collusion attack, when this user has not taken part, should be as low as possible (false positive probability).

US Patent Serial No. 5, 664, 018 discloses a watermarking process in which a plurality of copies of material items are marked with a digital watermark formed from a code word having a predetermined number of coefficients. The watermarked material item is for example an image. The apparatus for introducing the watermark transforms the image into the Discrete Cosine Transform (DCT) domain. The digital watermark is formed from a set of randomly distributed coefficients having a normal distribution. In the DCT domain each code word coefficient is added to a corresponding one of the DCT coefficients. The watermarked image is formed by performing an inverse DCT. A related publication entitled "Resistance of Digital Watermarks to Collusion Attacks", by J. Kilian, F. T. Leighton et al, published by MIT, July 27, 1998, provides a detailed mathematical analysis of this watermarking process to prove its resistance to attack.

Summary of Invention

According to an aspect of the present invention there is provided an encoding data processing apparatus for generating at least one marked copy of an original item of material by introducing one of a predetermined set of code words into a copy of the material item. The code word has a plurality of code word coefficients. The data processing apparatus includes an encoding processor operable to combine the code word coefficients with the material item. The plurality of code words of the set is derived from a first code word comprising a first plurality of coefficients. At least one other of the plurality of code words is generated from a cyclic shift of the first code word.

The present invention aims to provide a practical watermarking system, which utilises code words having coefficients which are randomly distributed as proposed as in US 5,664,018. In order to implement a practically useful system the number of uniquely identifiable code words in the set should be as high as possible. For a consumer distributed product such as a video or a film for display at a cinema, there should be in the order of a million or preferably tens of millions of code words in the set. As such, it will be appreciated that forming a correlation of each of the regenerated code words in the set of ten million and the recovered code word represents a considerable computational task. As such even for high performance computers, such a correlation would require an impracticably long time or at least an inconveniently long time. Embodiments of the present invention are provided with an advantage with respect to calculating the correlation values for the code words in the set. This is provided by forming at least some of the code words of the set by generating a first code word and generating other code words by cyclically shifting the first code word. As such the correlation values for all code words of the set can be calculated using a Fourier transform correlator. As will be explained, the Fourier transform correlator provides the correlation values for the set in one operation, substantially reducing the computational task.

According to an aspect of the present invention there is provided a data processing apparatus comprising a decoding processor operable to generate a recovered code word from a marked material item, and a detection processor operable to detect at least one code word from marked material item. The code word is detected from correlation values produced by correlating the recovered code word with each one of a plurality of regenerated code words. A code word is detected if the corresponding correlation value exceeds a predetermined threshold. The correlation value is formed for a plurality of the code words by

forming a Fourier transform of the recovered code word,

forming a Fourier transform of the first code word of said set,

forming the complex conjugate of one of the Fourier transform of the recovered code word and the Fourier transform of the regenerated code word,

forming intermediate product samples by multiplying each of said Fourier transform samples of said recovered code word and the corresponding Fourier transform samples of said first code word,

forming correlation samples by forming an inverse transform of said intermediate product samples, each of said correlation value samples providing the correlation value for one of said set of code words.

In preferred embodiments, the encoding processor is operable to permute the order in which the code word coefficients are combined with the material in accordance with a permutation code. Correspondingly in preferred embodiments the detecting data processor is arranged to reverse the permutation of either the re-generated code word coefficients or the recovered code word coefficients in order to perform the correlation values. Permuting the code word coefficients provides an advantage of reducing the likelihood of a successful collusion attack, which may increase by forming the code words from cyclically shifting the first code word.

Various further aspects and features of the present invention are defined in the appended claims.

Description of Preferred Embodiments

Watermarking System Overview

An example embodiment of the present invention will now be described with reference to protecting video images. The number of users to which the video images are to be distributed determines the number of copies. To each copy an identification code word is added which identifies the copy assigned to one of the users.

Video images are one example of material, which can be protected by embedding a digital code word. Other examples of material, which can be protected by embedding a code word, include software programs, digital documents, music, audio signals and any other information-bearing signal.

An example of an encoding image processing apparatus, which is arranged to introduce an identification code word into a copy of an original image, is shown in Figure 1. An original image *I* is received from a source and stored in a frame store 1. This original image is to be reproduced as a plurality of water marked copies, each of which is marked with a uniquely identifiable code word. The original image is passed to a Discrete Cosine Transform (DCT) processor 2, which divides the image into 8 x 8 pixel blocks and forms a DCT of each of the 8x8 pixel blocks. The DCT processor 2 therefore forms a DCT transformed image *V*.

In the following description the term "samples" will be used to refer to discrete samples from which an image (or indeed any other type of material) is comprised. The samples may be luminance samples of the image, which is otherwise, produce from the image pixels. Therefore, where appropriate the terms samples and pixels are inter-changeable.

The DCT image *V* is fed to an encoding processor 4. The encoding processor 4 also receives identification code words from an identification code word generator 8.

The code word generator 8 is provided with a plurality of seeds, each seed being used to generate one of the corresponding code words. Each of the generated code words may be embedded in a copy of the original image to form a watermarked image. The code word generator 8 is provided with a pseudo random number generator. The pseudo random number generator produces the code word coefficients to form a particular code word. In preferred embodiments the coefficients of the code

words are generated in accordance with a normal distribution. However, the coefficients of the code word are otherwise predetermined in accordance with the seed, which is used to initialise the random number generator. Thus for each code word there is a corresponding seed which is store in a data store 12. Therefore it will be understood that to generate the code word X^i, $seed_i$ is retrieved from memory 12 and used to initialise the random number generator within the code word generator 8.

In the following description the DCT version of the original image is represented as V, where;

$$V = \{v_i\} = \{v_1, v_2, v_3, v_4, \ldots\ldots\ldots\ldots v_N\}$$

and v_i are the DCT coefficients of the image. In other embodiments the samples of the image v_i could represent samples of the image in the spatial domain or in an alternative domain.

Each of the code words X^i comprises a plurality of n code word coefficients, where;

$$X^i = \{x_j^i\} = \{x_1^i, x_2^i, x_3^i, x_4^i, \ldots\ldots\ldots\ldots x_n^i\}$$

The number of code word coefficients n corresponds to the number or samples of the original image V. However, a different number of coefficients is possible, and will be set in dependence upon a particular application.

A vector of code word coefficients X^i forming the i-th code word is then passed via channel 14 to the encoder 4. The encoder 4 is arranged to form a watermarked image W^i by adding the code word X^i to the image V. Effectively, therefore, as represented in the equation below, each of the code word coefficients is added to a different one of the coefficients of the image to form the watermark image W^i.

$$W^i = V + X^i$$

$$W^i = v_1 + x_1^i, v_2 + x_2^i, v_3 + x_3^i, v_4 + x_4^i, \ldots\ldots\ldots\ldots, v_n + x_n^i$$

As shown in Figure 1, the watermarked images W^i are formed at the output of the image processing apparatus by an forming inverse DCT of the image produced at the output of the encoding processor 4 by the inverse DCT processor 18.

Therefore as represented in Figure 1 at the output of the encoder 4 a set of the watermarked images can be produced. For a data word of up to 20-bits, one of 10 000

000 code words can be selected to generate 10 million watermarked W^i versions of the original image I.

Although the code word provides the facility for uniquely identifying a marked copy W^i of the image I, in other embodiments the 20 bits can provide a facility for communicating data within the image. As will be appreciated therefore, the 20 bits used to select the identification code word can provide a 20 bit pay-load for communicating data within the image V.

The encoding image processing apparatus which is arranged to produce the watermarked images shown in Figure 1 may be incorporated into a variety of products for different scenarios in which embodiments of the present invention find application. For example, the encoding image processing apparatus may be connected to a web site or web server from which the watermarked images may be downloaded. Before downloading a copy of the image, a unique code word is introduced into the downloaded image, which can be used to detect the recipient of the downloaded image at some later point in time.

In another application the encoding image processor forms part of a digital cinema projector in which the identification code word is added during projection of the image at, for example, a cinema. Thus, the code word is arranged to identify the projector and the cinema at which the images are being reproduced. Accordingly, the identification code word can be identified within a pirate copy produced from the images projected by the cinema projector in order to identify the projector and the cinema from which pirate copies were produced. Correspondingly, a watermarked image may be reproduced as a photograph or printout in which a reproduction or copy may be made and distributed. Generally therefore, the distribution of the watermarked images produced by the encoding image processing apparatus shown in Figure 1 is represented by a distribution cloud 19.

Detecting Processor

A detecting image processing apparatus which is arranged to detect one or more of the code words, which may be present in an offending marked image is shown in Figure 2. Generally, the image processor shown in Figure 2 operates to identify one or more of the code words, which may be present in an offending copy of the image.

The offending version of the watermarked image W' is received from a source and stored in a frame store 20. Also stored in the frame store 24 is the original version of the image I, since the detection process performed by the image processor requires the original version of the image. The offending watermarked image W' and the original version of the image are then fed via respective connecting channels 26, 28 to a registration processor 30.

As already explained, the offending version of the image W' may have been produced by photographing or otherwise reproducing a part of the watermarked image W^i. As such, in order to improve the likelihood of detecting the identification code word, the registration processor 30 is arranged to substantially align the offending image with the original version of the image present in the data stores 20 and 24. The purpose of this alignment is to provide a correspondence between the original image samples I and the corresponding samples of the watermarked image W^i to which the code word coefficients have been added.

The effects of the registration are illustrated in Figure 3. In Figure 3 an example of the original image I is shown with respect to an offending marked version of the image W'. As illustrated in Figure 3, the watermarked image W' is offset with respect to the original image I and this may be due to the relative aspect view of the camera from which the offending version of the watermarked image was produced.

In order to recover a representation of the code word coefficients, the correct samples of the original image should be subtracted from the corresponding samples of the marked offending image. To this end, the two images are aligned. As shown in Figure 3, the registered image W'' has a peripheral area PA which includes parts which were not present in the original image.

As will be appreciated in other embodiments, the registration processor 30 may not be used because the offending image W' may be already substantially aligned to the originally version of the image I, such as, for example, if the offending version was downloaded via the Internet. Accordingly, the detecting image processor is provided with an alternative channel 32, which communicates the marked image directly to the recovery processor 40.

The registered image W'' is received by a recovery processor 40. The recovery processor 40 also receives a copy of the original image I via a second channel 44. The registered image W'' and the original image I are transformed by a DCT transform processor 46 into the DCT domain. An estimated code word X' is then formed by subtracting the samples of the DCT domain marked image V' from the DCT domain samples of the original image V as expressed by the following equations:

$$X' = V' - V$$

$$= v_1' - v_1, v_2' - v_2, v_3' - v_3, v_4' - v_4, \ldots\ldots\ldots, v_n' - v_n,$$

$$= x_1', x_2', x_3', x_4', \ldots\ldots\ldots\ldots x_n'$$

The output of the recovery processor 40 therefore provides on a connecting channel 50 an estimate of the coefficients of the code word which is to be identified. The recovered code word X' is then fed to a first input of a correlator 52. The correlator 52 also receives on a second input the regenerated code words X^i produced by the code word generator 54. The code word generator 54 operates in the same way as the code word generator 8 which produces all possible code words of the set, using the predetermined seeds which identify uniquely the code words from a store 58.

The correlator 52 forms n similarity $sim(i)$ values. In one embodiment, the similarity value is produced by forming a correlation in accordance with following equation:

$$sim(i) = \frac{X^i \cdot X'}{\sqrt{X^i \cdot X'}} = \frac{x_1^i \cdot x_1' + x_2^i \cdot x_2' + x_3^i \cdot x_3' + \ldots\ldots + x_n^i \cdot x_n'}{\sqrt{x_1^i \cdot x_1' + x_2^i \cdot x_2' + x_3^i \cdot x_3' + \ldots\ldots + x_n^i \cdot x'}}$$

Each of the n similarity values $sim(i)$ is then fed to a detector 60. The detector 60 then analyses the similarity values $sim(i)$ produced for each of the n possible code words. As an example, the similarity values produced by the correlator 52 are shown in Figure 4 with respect to a threshold TH for each of the possible code words. As shown in Figure 4, two code words are above the threshold, 2001, 12345. As such, the detecting processor concludes that the watermarked version associated with code word 2001 and code word 12345 must have colluded in order to form the offending image. Therefore, in accordance with a false positive detection probability, determined from the population size, which in this case is 10 million and the watermarking strength α ,

the height of the threshold *TH* can be set in order to guarantee the false detection probability. As in the example in Figure 4, if the similarity values produced by the correlator 52 exceed the threshold then, with this false positive probability, the recipients of the marked image are considered to have colluded to form the offending watermarked version of the image W^i.

The following sections illustrate advantages and features of the operation of the watermarking system illustrated in Figures 1 and 2.

Registration

The process of aligning the offending marked version of the image with the copy of the original image comprises correlating the samples of the original image with respect to the marked image. The correlation is performed for different shifts of the respective samples of the images. This is illustrated in Figure 5.

Figure 5A provides an illustration of discrete samples of the original image *I*, whereas Figure 5B provides an illustration of discrete samples of the offending watermarked image *W'*. As illustrated in the Figures 5A and 5B, the sampling rate provides a temporal difference between samples of *dt*. A result of shifting each of the sets of samples from the images and correlating the discrete samples is illustrated in Figure 5C.

As shown in Figure 5C, for a shift of between 6 and 7 samples, the correlation peak is highest. The offending watermarked image is therefore shifted by this amount with respect to the original image to perform registration.

Fourier Decoding

As explained, with reference to Figures 1 and 2, the watermarking system can provide a facility for generating 10 million watermarked versions of an original image. This is effected using a 20-bit watermark value. However, as explained, in order to detect the presence of one of the code words in an offending watermarked image, the detecting image processor must correlate each of the possible code words in the set of 10 million code words with respect to a recovered code word from the image. As will be appreciated, this represents a considerable computational task.

A correlator embodying the present invention provides a significant advantage in reducing the computational effort and therefore the time taken to detect the presence of a code word in an offending watermarked image. A correlator in accordance with the embodiment of the present invention is illustrated in Figure 6. The correlator shown in Figure 6 takes advantage of an alternative technique for calculating the correlation sum shown above. In accordance with this technique the correlation sum is calculated in accordance with the following equation:

$F^{-1}[F(X')F(X^{(i)})^*]$, where $F(A)$ is the Fourier transform of A and $F^{-1}(A)$ is the inverse Fourier transform of A.

The corrolator 52 shown in Figure 6 therefore comprises a first Fourier transform processor 100, and a second Fourier transform processor 102. Fourier transform processors 100, 102 may be implemented using Fast Fourier transform algorithms. The second Fourier transform processor 102 also forms the complex conjugate of the Fourier transform of the regenerated code word X^i. The Fourier transform of the recovered code word X' and the complex conjugate of the Fourier transform of the regenerated code word X^i are fed to first and seconds inputs of a multiplier 110. The multiplier 110 multiplies the respective samples from each of the Fourier transform processors 100, 102 and feeds the multiplied samples to an inverse Fourier transform processor 112. At the output of the correlator an inverse Fourier transform of the multiplied signals samples is formed.

As will be appreciated, the implementation of the correlator 52 shown in Figure 6 provides an advantage in terms of time taken to compute the correlation for the n sample values of the regenerated code word X^i and the recovered code word X'. This is because the Fourier processors 100, 102, 112 can be formed from FFT integrated circuits such as, for example, are available as ASICS. Furthermore, the inverse Fourier transform provided at the output of the corrolator 52 provides n similarity values $sim(i)$ corresponding to n correlation sums. However, in order to utilise the properties of the corrolator 52, shown in Figure 6 the code words are arranged to be generated by cyclically shifting one code word generated $X^{(1)}$ using a particular seed for the random number generator. This is illustrated below. As shown below, the first code word $X^{(1)}$ is represented as values x_1 to x_n which corresponds to the pseudo randomly produced

numbers from the code word generator 8. However, the second code word $X^{(2)}$ is produced by performing a cyclic shift on the first code word $X^{(1)}$. Correspondingly, each of the other code words are produced by correspondingly cyclically shifting further the code word $X^{(1)}$ until the n-th code word is a code word shifted by n-1 positions.

$$X^{(1)} \rightarrow (x_1, x_2, x_3, x_4 \ldots\ldots\ldots\ldots, x_{n-1}, x_n)$$

$$X^{(2)} \rightarrow (x_2, x_3, x_4 \ldots\ldots\ldots\ldots, x_{n-1}, x_n, x_1)$$

$$X^{(3)} \rightarrow (x_3, x_4 \ldots\ldots\ldots\ldots, x_{n-1}, x_n, x_1, x_2)$$

- - - - - - - - - - - -

$$X^{(n)} \rightarrow (x_n, x_1, x_2, x_3, x_4, \ldots\ldots\ldots\ldots x_{n-2}, x_{n-1})$$

By using this set of code words to form part of, or the whole of, the set of code words produced by the encoding image processor, the Fourier transform correlator 52 can be used to generate in one operation all similarity values for all of the n code words. Therefore, as illustrated above, the corresponding shift of 1 to n of the original code word provides the n similarity values *sim(i)*, and as illustrated in Figure 4, for at least one of the code words, a large similarity value *sim(i)* is produced. Therefore, as will be appreciated the correlator 52 only receives one regenerated code word corresponding to first code word $X^{(1)}$ to form the similarity values for the set of n code words as illustrated in Figure 4.

As will be appreciated from the above explanation, if the code word contains N samples, then only N unique cyclic shifts are possible. Therefore, if the required population of code words is p, which is greater than N, then several base watermarks will be required. Each base watermark can be cyclically shifted to produce N unique code words.

If the watermarked image forms one of a plurality of images in, for example, a video sequence, then the same code word will be added to each of the images. As such, once the suspected code word has been identified using the Fourier transform corrolator illustrated in Figure 6, then a subsequent correlation can be formed using the full correlation sum *sim(i)* as explained above. However, because the suspected code

word has already been identified, then the correlation only needs to be performed once for the code word identified by the Fourier transform correlator shown in Figure 6.

As will be appreciated, instead of forming the conjugate of the Fourier transform of the regenerated first code word X^1, the conjugate of the Fourier transform of the recovered code word could be formed. This is expressed by the second alternative of the Fourier transform correlator shown below:

$$F^{-1}[F(X')^* F(X^{(1)})]$$

Accordingly the conjugate of one of the Fourier transform of the recovered code word and the Fourier transform of the regenerated code word is formed by the Fourier transform processors 100, 102.

Secret Permutation of Code Words

One disadvantage of forming a code word from a cyclic shift of a first code word X^1 is that the security of the watermark may be compromised. This is because under a collusion attack two watermarked images are compared. If the same code word has been added to each image, with only a cyclic shift with respect to two versions of the same code word, an attacker may be more likely to identify the differences between the two marked material items and therefore identify the code word. With knowledge of the code word an attacker may either remove the watermark or alter the watermark to falsely implicate another.

In order to reduce the likelihood of a successful collusion attack, the order of each of the code word coefficients of each of the cyclically shifted code words is randomly permuted in accordance with a secret permutation code π. The permutation of the code word coefficients remains secret from the recipients of the marked images. Accordingly the likelihood of a successful collusion attack is reduced by an increase in the difficulty presented to a collusion attacker of identifying a correlation between two marked images.

At the detecting data processor the secret permutation code π will be known. In the detecting data processor, either the code word re-generator or the recovery processor 40 is operable to reverse the permutation π^{-1} of either the re-generated code word coefficients or the recovered code word coefficients in order to perform the correlation. The operation of the encoding data processor of Figure 1 and the detecting

data processor of Figure 2 is therefore as presented in a flow diagrams in Figures 7 and 8 respectively.

Code Word Generation

A further advantageous aspect of the embodiment shown in Figures 1 and 2 is provided by generating the seed of the random number from which the code word is produced from the source image samples. This is affected by analysing the DCT coefficients of the image to be watermarked and from these coefficients, generating the seed to be used to generate the code word. This can be effected, for example, by using a hashing algorithm known to those skilled in the art as "secure hashing algorithm 1" (sha-1). This algorithm forms an ANSI standard (ANSI x9.30-2). This algorithm is referred to in a book entitled "Handbook of applied cryptography" by A.J. Menezes. As such the seed from the random number can be generated and determined in the encoding image processor and the detecting image processor from the DCT coefficients.

Other Applications

In addition to the above-mentioned applications of the encoding data processing apparatus of the watermarking system to a cinema projector and to a web server, other applications are envisaged. For example, a receiver/decoder is envisaged in which received signals are watermarked by introducing code words upon receipt of the signals from a communicating device. For example, a set top box is typically arranged to receive television and video signals from a "head-end" broadcast or multi-cast device. As will be appreciated in this application, the encoding data processing apparatus forms part of the set top box and is arranged to introduce watermark code words into the video signals as the signals are received and decoded. In one example embodiment, the watermark code word is arranged to uniquely identify the set top box which receives and decodes the video signals.

In a further embodiment a digital cinema receiver is arranged to receive a digital cinema film via a satellite. The receiver is arranged to receive signals representing the digital cinema film and to decode the signals for reproduction. The receiver includes an encoding data processing apparatus, which introduces a

watermark code word into the decoded film signals. The watermark code word is provided, for example, to uniquely identify the cinema receiving the film signals.

A further example embodiment may comprise a digital camera or camcorder or the like which includes a memory and a memory controller. An encoding data processing apparatus according to an embodiment of the present invention is arranged to introduce a watermark code word stored in the memory into video signals captured by the camera. According to this embodiment, the encoding data processing apparatus does not include a code word generator because the code word is pre-stored in the memory. Under the control of the memory controller the code word stored in the memory is embedded into the video signals, uniquely or quasi-uniquely identifying the video signals.

In a further embodiment, an encoding data processing apparatus according to an embodiment of the invention is operable encoded a sequence of watermark code words into different frames of digital images forming a continuous or moving picture. The code words may be related to one another and may be used to identify each of the images separately.

Various further aspects and features of the present invention are defined in the appended claims. Various modifications can be made to the embodiments herein before described without departing from the scope of the present invention.

4 Brief Description of Drawings

Figure 1 is a schematic block diagram of an encoding image processing apparatus;

Figure 2 is a schematic block diagram of a detecting image processing apparatus;

Figure 3A is a representation of an original image, Figure 3B is a representation of a marked image and Figure 3C is the marked image after registration;

Figure 4 is a graphical representation of an example correlation result for each of a set of N code words;

Figure 5A is a graphical representation of samples of the original image I, Figure 5B is a graphical representation of samples of the watermarked image W'; Figure 5C is a graphical representation of correlation results for the original image and the watermarked image with respect to discrete sample shifts;

Figure 6 is a schematic block diagram of a correlator forming part of the detecting data processing apparatus shown in Figure 2;

Figure 7 is a flow diagram of a process for forming watermarked images performed by the encoding image data processor; and

Figure 8 is a flow diagram of a process for identifying a watermark from a received marked copy of the image performed by the detecting data processor of Figure 2;

1 Abstract

A watermarking system comprises an encoding data processor operable to generate at least one marked version of an original item of material by introducing one of a predetermined set of code words into a copy of the original material item. The apparatus comprises a code word generator operable to provide the code word comprising a plurality of code word coefficients, and an encoding processor operable to combine the code word coefficients with the material. The set of code words is formed by cyclically shifting a first code word. An advantage is thereby provided to a detecting data processor, which can be arranged to form the correlation values for all code words, formed by shifting the first code word, using a Fourier transform correlator. As a result a time taken to detect a code word present in a marked material item can be considerably improved. The watermarking system finds particular application in identifying a point of distribution of pirate copies of video material generated by capturing the watermarked image, using, for example, a camcorder in a cinema.

2 Representative Drawing

[Fig 7]

【図１】

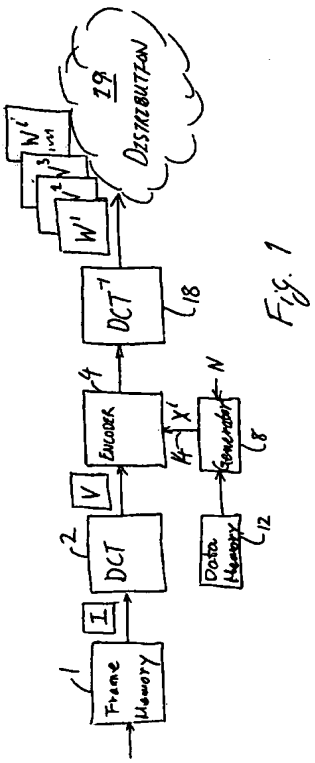


Fig. 1

【図２】

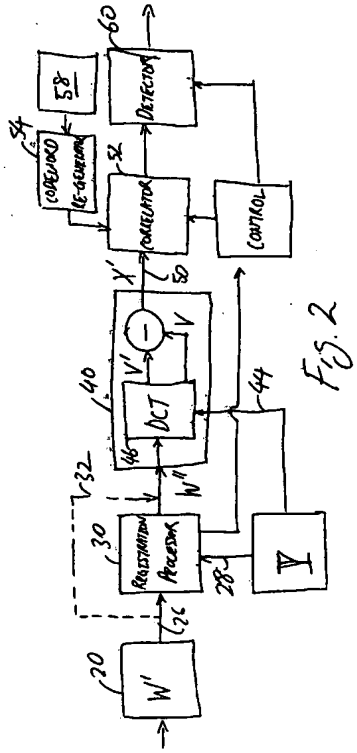


Fig. 2

【図３】

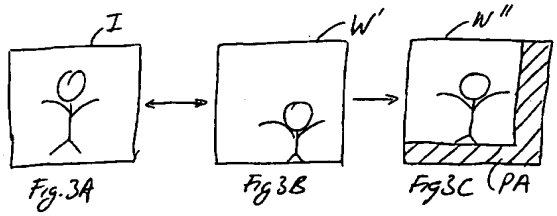


Fig.3

【図４】

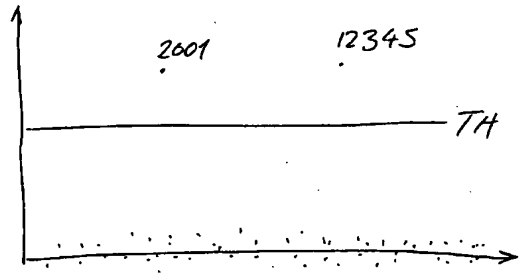


Fig.4

【図５】

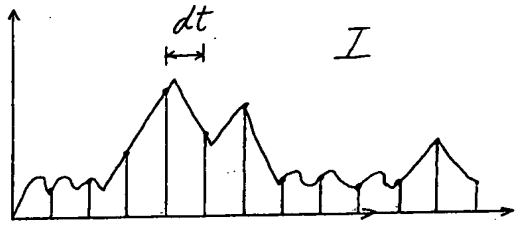


Fig.5A

【図６】

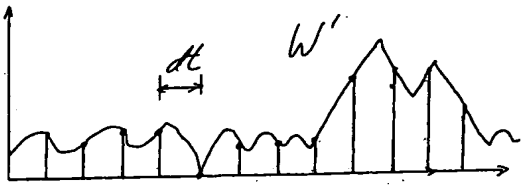


Fig 5B

【図７】

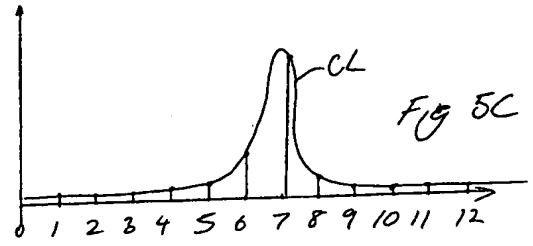


Fig 5C

【図８】

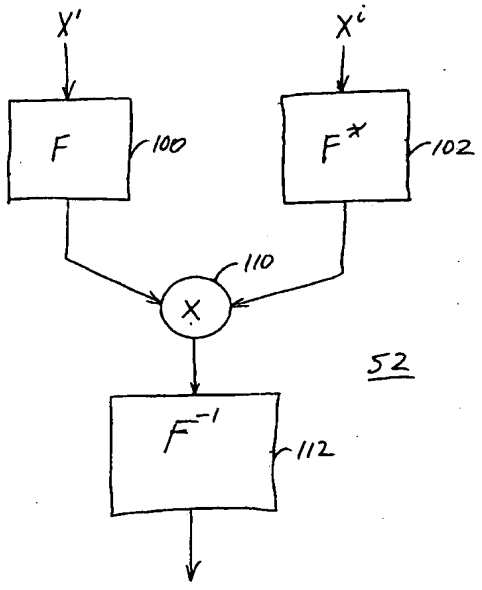


Fig.6

【図９】

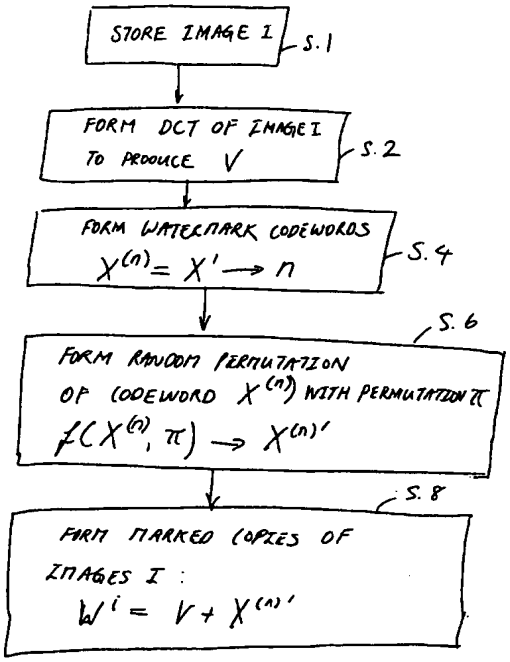


Fig. 7

【図１０】

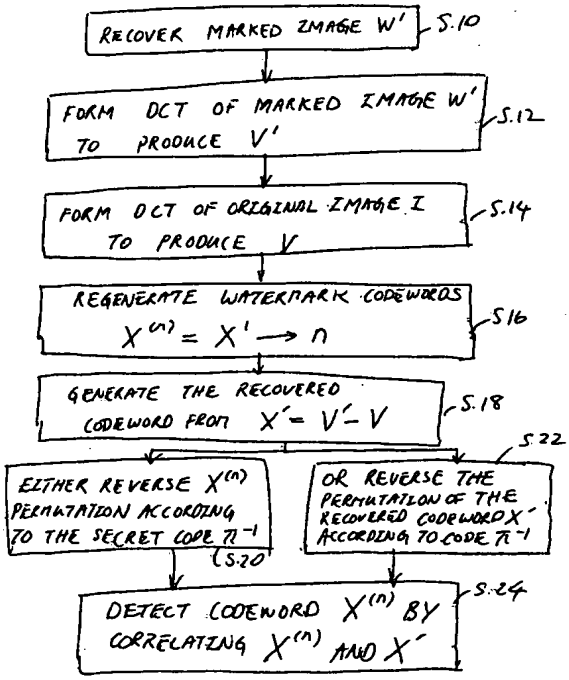


Fig. 8